



# 3Com® X Family Command Line Interface Reference



**X5 (25-user license) – 3CRTPX5-25-96**  
**X5 (unlimited license) – 3CRTPX5-U-96**  
**X506 – 3CRX506-96**

**Version 2.5.1**

Part Number TECHD-178 Rev B01  
Published April 2007

<http://www.3com.com/>



**3Com Corporation**  
**350 Campus Drive**  
**Marlborough, MA**  
**01752-3064**

Copyright © 2005–2007, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms, or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hardcopy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

#### **UNITED STATES GOVERNMENT LEGENDS:**

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

**United States Government Legend:** All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, TippingPoint, the TippingPoint logo, and Digital Vaccine are registered trademarks of 3Com Corporation or one of its subsidiaries.

OpenView is a trademark of Hewlett-Packard Development Company. Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries. Oracle is a registered trademark of Oracle Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

# Contents

## Contents iii

### About This Guide v

Welcome to the X Family CLI	v
Target Audience	vi
Conventions	vi
Related Documentation	viii
Customer Support	viii

### Chapter 1: X Family Startup Configuration 1

Overview	1
Initial Configuration	1
Configuration Categories	2
Initiating the Setup Wizard	4
Account Security Level	4
Super-User Data	5
Host Configuration	7
Timekeeping Options	7
Network Deployment Configuration	9
Virtual Interface Configuration	9
Basic Security Zone Configuration	10
Assigning Zones to Virtual Interfaces	11
Configuring DNS Settings	11
Setup Firewall Rules	12
Enabling SMS Configuration	13
Web, CLI, and SNMP Server Options	14
NMS Settings	16
Restrict SMS	16
Additional Configuration	16
After the Setup Wizard	20

### Chapter 2: Command Reference 21

Overview	21
----------	----

!	28
alias	28
boot	29
bugreport	30
clear	31
cls	33
configure	33
debug	81
exit	81
halt	82
help	82
high-availability	82
history	83
logout	83
ping	84
quarantine	85
quit	85
reboot	85
setup	86
show	86
snapshot	118
traceroute	118
traffic-capture	119
tree	120
who	121
whoami	122

## **Chapter 3: Navigation 123**

Overview	123
Logging in to the CLI	123
Navigation	124
Console Settings	128

## **Index 131**

# About This Guide

*Explains who this guide is intended for, how the information is organized, where information updates can be found, and how to obtain customer support if you cannot resolve a problem.*

## Welcome to the X Family CLI

Welcome to the X family *Command Line Interface (CLI)*. The CLI is the interface for issuing commands via a command line prompt for the X family device. You use this interface to configure, monitor, and report on the X family devices in your network.

This section covers the following topics:

- [“Target Audience” on page vi](#)
- [“Conventions” on page vi](#)
- [“Related Documentation” on page viii](#)
- [“Customer Support” on page viii](#)

# Target Audience

This guide is intended for super-users and administrators who manage one or more X family devices.

## Knowledge, Skills, and Abilities

This guide assumes you, the reader, are familiar with general networking concepts and the following standards and protocols:

- TCP/IP
- UDP
- ICMP
- Ethernet
- Network Time Protocol (NTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)

# Conventions

This guide follows several procedural and typographical conventions to provide clear and understandable instructions and descriptions. These conventions are described in the following sections.

This book uses the following conventions for structuring information:

- [Cross References](#)
- [Typeface](#)
- [Messages](#)

## Cross References

When a topic is covered in depth elsewhere in this guide, or in another guide in this series, a cross reference to the additional information is provided. Cross references help you find related topics and information quickly.

### Internal Cross References

This guide is designed to be used as an electronic document. It contains cross references to other sections of the document that act as hyperlinks when you view the document online. The following text is a hyperlink: [Messages](#).

### External Cross References

Cross references to other publications are not hyperlinked. These cross references will take the form: see <chapter name> in the *Publication Name*.

## Typeface

This guide uses the following typographical conventions:

<b>bold</b>	used for commands or parameters, which must be entered exactly as shown.
<i>light font</i>	used for variables, for which you supply a value.
<b>brackets []</b>	used to indicate an optional element.
<b>&lt;1   2 &gt;</b>	angle brackets and vertical bars are used to indicate a choice that must be made.
<i>Italic</i>	used for guide titles, variables, and important terms.
<a href="#">Hyperlink</a>	used for cross references in a document or links to a Web site.

## Messages

Messages are special text that are emphasized by font, format, and icons. There are four types of messages in this guide:

- [Warning](#)
- [Caution](#)
- [Note](#)
- [Tip](#)

A description of each message type with an example message follows.

### Warning

Warnings tell you how to avoid physical injury to people or equipment. For example:.



**WARNING:** The push-button on/off power switch on the front panel of the server does not turn off the AC power. To remove AC power from the server, you must unplug the AC power cord from either the power supply or the wall outlet.

### Caution

Cautions tell you how to avoid a serious loss that could cause physical damage such as the loss of data, time, or security. You should carefully consider this information when determining a course of action or procedure. For example:



**CAUTION:** You should disable password caching in the browser you use to access the LSM. If you do not disable password caching in your browser, and your workstation is not secured, your system security may be compromised.

## Note

Notes tell you about information that might not be obvious or that does not relate directly to the current topic, but that may affect relevant behavior. For example:



**Note:** Some command examples in this document are split across several lines due to space constraints; however, you must enter them on a single line (with no carriage returns).

## Tip

Tips are suggestions about how you can perform a task more easily or more efficiently. For example:



**Tip:** You can collect firewall statistics using **configure terminal firewall monitor**.

## Related Documentation

The X family devices have a full set of documentation. These publications are available in electronic format on CD. For the most recent updates, check the Threat Management Center (TMC) web site at <https://tmc.tippingpoint.com>.

## Customer Support

We are committed to providing quality customer support to all customers. A customer is provided with detailed customer and support contact information. For the most efficient resolution of your problem, please take a moment to gather some basic information from your records and from your system before contacting customer support.

Information	Location
Your X family device serial number	You can find this number in the LSM in the <i>System Summary</i> page, on the shipping invoice that came with the device, or on the bottom of the device.
Your TOS version number	You can find this information in the LSM in the <i>System Summary</i> page, or by using the CLI <code>show version</code> command.
Your X family system boot time	You can find this information in the LSM in the <i>System Summary</i> page.

## Contact Information

Please address all questions regarding the software to your authorized representative.



# X Family Startup Configuration

*The X family device is a high-speed, comprehensive security system. This section describes the steps required to start managing the X family device.*

## Overview

You must complete basic configuration of the X family device to pass traffic in the default configuration. The X Family Setup Wizard provides a convenient way for you to enter the necessary configuration data when you install a new device on your network, or when you move or reconfigure a device within your network. Refer to the following documents for hardware installation:

- *Quick Start Guide*
- *Hardware Installation and Safety Guide*

For the most recent updates, check the Threat Management Center (TMC) website. The Customer Support phone number is 1-866-681-8324.

## Initial Configuration

You can perform initial configuration on the X family device with OBE Setup Wizard or with the CLI Setup Wizard.

### The OBE Setup Wizard

The OBE Setup Wizard runs when you first connect to the device through the Local Security Manager (LSM) with your web browser. The LSM is a web-based GUI for managing one X family device. The

LSM provides HTTP and HTTPS (secure management) access. This access requires one of the following browsers:

- Microsoft Internet Explorer 6.0 or later
- Firefox 1.5 or later
- Mozilla 1.7 or later
- Netscape 8.1 or later

Using the LSM, you have a graphical display for reviewing, searching, and modifying settings. The GUI interface also provides graphical reports for monitoring the device traffic, triggered filters, and packet statistics.

For more information about using the OBE Setup Wizard to configure the device, refer to the *Quick Start Guide* for the X family device model. For more information about the LSM, refer to the *Local Security Manager User's Guide*.

## The CLI Setup Wizard

The Setup Wizard runs automatically on a console via a serial port connection when you first boot the X family device. You can also run the setup wizard from the Command Line Interface (CLI) at any time by entering the `setup` command.

This chapter describes the initial configuration process with the CLI Setup Wizard.

## Configuration Categories

The CLI Setup Wizard runs a series of short interactive dialogs to set several basic configuration variables on the X family device. The Out-of-the-Box Terminal Setup Wizard runs when the setup wizard is activated for the first time or at another time with the `setup` command. This wizard is run on a serial port connected system, such as a workstation and laptop.

After you run the setup wizard using a serial terminal, you can further configure the device using subsequent setup commands through the CLI. See [“Additional Configuration” on page 16](#) for details.

The Out-of-the-Box Setup Wizard runs on a workstation or laptop connected to the serial port of the device. The configuration dialogs are shown in the following table:

**Table 1–1: Out-of-the-Box Terminal Setup Wizard Configuration Settings**

Out-of-the-Box Setup	Subsequent Setups	Settings
Account Security Level	—	account security level
Super-user Data	—	super-user login name super-user password

**Table 1–1: Out-of-the-Box Terminal Setup Wizard Configuration Settings (Continued)**

Out-of-the-Box Setup	Subsequent Setups	Settings
Timekeeping Options	Timekeeping Options	NTP or CMOS clock time zone daylight saving time NTP: up to four time servers or peers CMOS clock: date time
Modify interfaces	Modify virtual interfaces	IP allocation settings Subnet mask NAT enable/disable
Modify security zones	Modify security zones	Create zone Allocate ports to zones Assign zones to interfaces Enable DHCP on an internal interface
Setup basic firewall rules	Modify firewall rules	View default firewall rules Allow all internal zones access to the Internet Apply web filtering Allow management of device from WAN
Enable SMS Configuration	Enable SMS Configuration	enable SMS configuration select the SMS device that will configure the X family device
Web, CLI, and SNMP Server Options	Web, CLI, and SNMP Server Options	HTTPS or HTTP SSH SNMP
NMS Configuration	NMS Configuration	NMS IP address and port NMS community string
Restricted SMS Access	Restricted SMS Access	SMS IP address
—	Ethernet Ports	enable ports line speed duplex setting auto negotiation

**Table 1–1: Out-of-the-Box Terminal Setup Wizard Configuration Settings (Continued)**

Out-of-the-Box Setup	Subsequent Setups	Settings
—	Default E-Mail Contact	TO: email FROM: email email domain SMTP server IP email aggregation period
—	Remote Syslog Server	IP address

## Initiating the Setup Wizard

When the Setup Wizard runs, the following screen displays:

```
Welcome to the TippingPoint Technologies Initial Setup wizard.
Press any key to begin Initial Setup Wizard.
```

When you press a key, you see the following:

```
You will be presented with some questions along with default values in
brackets[ ]. Please update any empty fields or modify them to match your
requirements. You may press the ENTER key to keep the current default
value. After each group of entries, you will have a chance to confirm
your settings, so don't worry if you make a mistake.
```

Continue to the following section for instructions on account security.



**Tip:** During initial setup, use the Ctrl-H key combination to erase characters you have already typed. Ctrl-H deletes from right to left one character at a time.

## Account Security Level

The Security Level dialog sets the security level settings that restrict user names and passwords. The default security level is Level 2, but you have the option to select any of the three available levels:

**Table 1–2: Security Levels**

Level	Description
Level 0	User names cannot contain spaces. Passwords are unrestricted.
Level 1	User names must contain at least 6 characters without spaces. Passwords must contain at least 8 characters without spaces.

**Table 1–2: Security Levels**

Level	Description
Level 2	Includes Level 1 restrictions and requires the following: <ul style="list-style-type: none"> <li>• 2 alphabetic characters</li> <li>• 1 numeric character</li> <li>• 1 non-alphanumeric character (special characters such as ! ? and *).</li> </ul>

**Example**

There are three security levels for specifying user names and passwords:

Level 0: User names and passwords are unrestricted.

Level 1: Names must be at least 6 characters long; passwords at least 8.

Level 2: In addition to level 1 restrictions, passwords must contain:

- at least 2 alpha characters
- at least 1 numeric character
- at least 1 non-alphanumeric character

Please specify a security level to be used for initial super-user name and password creation. As super-user, you can modify the security level later on via Command Line Interface (CLI) or Local Security Manager (LSM).

Security level [2]:

## Super-User Data

The Super-User Data dialog sets the super-user login name and password. The login name and password must meet the restrictions of the security level that you set in the Security Level dialog. The following tables list examples of valid and invalid login names and passwords.

**Table 1–3: Login Name Examples**

Valid Login Names	Invalid Login Names
fjohnson	fredj (too short in Levels 1 and 2, valid for Level 0)
fredj123	fred j 123 (contains spaces)
fredj-123	fj123 (too short)
fredj-*123	fj 123 (contains spaces)

**Table 1–4: Password Examples for Level 2 Security**

Valid Passwords	Invalid Passwords
my-pa55word	my-pa55 (too short)

**Table 1–4: Password Examples for Level 2 Security**

Valid Passwords	Invalid Passwords
my-b1rthday	mybirthday (must contain numeric)
myd*g'snam3	mydogsnam3 (must contain a non-alphanumeric character)

### Example

In this example, the password is presented in italics. In the actual dialog, the password would not be visible.

```
Please enter a user name that we will use to create your super-
user account. Spaces are not allowed.
```

```
Name: superuser
Do you wish to accept [superuser] <Y,[N]>:Y
```

```
Please enter your super-user account password: root--00
Verify password: root--00
Saving information...Done
```

```
Your super-user account has been created.
```

```
You may continue initial configuration by logging into your
device. After logging in, you will be asked for additional
information.
```

## Host Configuration

The Host Configuration dialog configures the host name and host location. You also have the option to configure the host management port.



**CAUTION:** Do not configure the host management port unless you have been specifically instructed to do so by technical support.

### Example

In this example, the host management port is not configured, and the host name is set as **device11** in the location **lab**.

```
The host management port is used to configure and monitor this device via
a network connection (e.g., a web browser).
```

```
Have you been directed by technical support to configure
the management port? <Y,[N]>:N
Enter Host Name [myhostname]: device11
Enter Host Location [room/rack]: lab
```

```
Host Name: device11
Host Location: lab
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: A
```

## Timekeeping Options

The Timekeeping Options dialog configures the X family device clock. You can configure the following options.

### Time Zone

The time zone option calculates and shows the local time. System logs are kept in Universal Time (UTC), but the device calculates local time for display purposes. Entering the proper time zone enables the device to display local time properly.

### Daylight Saving Time

The daylight saving time option enables and disables the calculation of time based on the time of year.

### NTP

The X family device can keep time using its internal CMOS clock or it can use a Network Time Protocol (NTP) server.



**Note:** Use the **show ntp session** and **sshow stp status** commands to inspect the operation of the NTP protocol.

### NTP Server

Configuring a host as an NTP server causes the X family device to query that host to obtain information on the current time. If multiple time servers are specified, the device aggregates data from all available servers to calculate the best time estimate. Providing multiple sources improves both the reliability and accuracy of the time data.

### NTP Peer

Configuring a host as an NTP peer causes the X family device to both send time information to and receive time information from the host. This allows multiple devices to mutually exchange time information, allowing for a higher resilience against the failure of one or more time servers.

### Date and Time

If you are not using NTP, you must specify the current date and time.

### Example

In this example, the time zone is set to Central Standard Time (CST), Daylight Saving Time changes are enabled, and NTP is not enabled. The default date is accepted, and the current time is entered manually:

```
Timekeeping options allow you to set the time zone, enable or
disable daylight saving time, and configure or disable NTP.

Would you like to modify timekeeping options? <Y,[N]>: y

Enter time zone or '?' for complete list [GMT]: CST
Automatically adjust clock for daylight saving changes? [Yes]: N
Do you want to enable the NTP client? [No]: N
Enter date <YYYY-MM-DD> [2006-06-09]:
Enter time <HH:MM:SS> in 24 hour notation [09:02:40]: 08:02:00

TimeZone: CST
DST enabled: No
NTP enabled: No
Date: 2006-06-09
Time: 08:02:00
```

```
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: A
```

## Network Deployment Configuration

The Network Deployment Configuration dialog selects the type of network deployment that the X family device will use. The following deployments are available:

- **Routed mode:** All IP subnets are unique, and addressees that traverse to the WAN zone may be subject to Network Address Translation (NAT).
- **NAT mode:** Hosts in the LAN zone run in a private IP address range, and hosts in the WAN zone run in a public IP address range. Addressees that traverse to the WAN zone may be subject to Network Address Translation (NAT).
- **Transparent (Layer 2) mode:** Firewalls are enforceable between security zones, but all zones are in the same broadcast domain.

NAT mode and Routed mode require internal and external virtual interfaces (VIs). The device has a single internal VI and a single external VI configured by default. Virtual Interface Configuration is discussed in detail in [“Virtual Interface Configuration” on page 9](#).

### Example

```
The X-Series device may be configured into a number of well known
network deployments.
```

```
Would you like to modify the network deployment mode? <Y,[N]>:y
```

```
Please choose a network deployment option:
```

- ```
1) Routed mode
2) NAT mode
3) Transparent (layer 2) mode
```

```
Please Select []: 1
```

## Virtual Interface Configuration

The virtual interface dialog of the initial setup wizard modifies the configuration of the internal and external interfaces and includes IP allocation, IP subnet, default gateway, and enabling or disabling NAT.

### Example

In this example, the default interface IP addresses are reviewed and accepted:

```
Virtual interfaces define how this device integrates with the IP layer 3
network. You must configure one virtual interface for every IP subnet that is
directly connected to the X-Series device. For example, you need one for the WAN
connection (external virtual interface) and one for every directly connected
network subnet (internal virtual interfaces).
```

```
Would you like to modify virtual interfaces? <Y,[N]>:y
```

```

Virtual interfaces:
Id Type      Mode   IP Address      Subnet Mask      NAT
1  internal static 192.168.1.254   255.255.255.0    external-ip
2  external dhcp  10.0.1.200      255.255.255.0    disable
3  <empty>
4  <empty>
5  <empty>
6  <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]:
a

```

## Basic Security Zone Configuration

The Security Zone dialog modifies the basic configuration of security zones, which divide your network into logical security domains. Network traffic between security zones is routed and scanned by the firewall and the IPS policies that you create.

In the setup process, you can assign security zones to different ports. You can change the zone configuration at any time afterwards.

### Example

In this example, a new security zone called **MyZone** is created:

Security zones enable you to section your network logically into security domains. As network traffic travels between zones, it is routed and security-scanned by the firewall and IPS according to the policies you define. You need to create security zones that naturally map onto your intended network security boundaries. A security zone may or may not be connected (mapped) to a virtual interface.

```

Would you like to modify security zones? <Y,[N]>:y
Security zones:
#      Zone name      Ports
1      LAN            1
2      VPN            None
3      WAN            6
4      <empty>
5      <empty>
6      <empty>
7      <empty>
8      <empty>
9      <empty>
10     <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]:
c
Enter the number of the entry you want to change []: 2
Zone Name [LAN2]: MyZone
Network port (0 for None) [0]: 1

*** WARNING: Accepting this change will move port 1 from "LAN"
to "VPN".
***

```

```

Security zones:
#      Zone name      Ports
1      LAN            None
2      VPN            1
3      WAN            6
4      <empty>
5      <empty>
6      <empty>
7      <empty>
8      <empty>
9      <empty>
10     <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]:
a

```

## Assigning Zones to Virtual Interfaces

The Modify Security Zones Mapping to Virtual Interfaces dialog maps existing zones to existing interfaces.

### Example

```

Would you like to modify security zone to Virtual Interfaces mapping? <Y,[N]>:y

Virtual interface to security zone mapping:
Id Type      Zones  Mode      IP Address      Subnet Mask
1  internal  LAN    static    192.168.1.254 255.255.255.0
                VPN
2  external  WAN    dhcp

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: c
Enter the number of the entry you want to change []: 1
Enter [A]dd, [R]emove, or [E]xit without saving [E]: r
Zone name []: LAN

Virtual interface to security zone mapping:
Id Type      Zones  Mode      IP Address      Subnet Mask
1  internal  VPN    static    192.168.1.254 255.255.255.0
2  external  WAN    dhcp

Enter [A]ccept, [C]hange or [E]xit without saving [C]: a

```

## Configuring DNS Settings

The Domain Name Services (DNS) dialog configures DNS settings. By default, the X family device acquires DNS settings using DHCP. You can use a custom DHCP server or specify a static address.

### Example

DNS (Domain Name Service) is a system which translates computer hostnames to IP addresses. The X-Series device requires DNS configuration in order to perform web filtering.

```

Would you like to configure DNS? <Y,[N]>:y

Would you like to use the DNS configuration obtained from the
WAN connection ? <[Y],N>:n
Enter DNS Server 1 IP Address (0.0.0.0 to clear): []: 10.0.0.1
Enter DNS Server 2 IP Address (0.0.0.0 to clear): []: 10.0.0.2
Enter DNS Server 3 IP Address (0.0.0.0 to clear): []:
Enter DNS Search Domain 1 (" to clear): []: example.com
Enter DNS Search Domain 2 (" to clear): []:
Enter DNS Search Domain 3 (" to clear): []:

DNS settings manually configured.

DNS Server 1: 10.0.0.1
DNS Server 2: 10.0.0.2
DNS Server 3:
DNS Domain 1: example.com
DNS Domain 2:
DNS Domain 3:

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a

```

## Setup Firewall Rules

The Setup Firewall Rules dialog will reset all firewall rules back to the factory defaults and then enable you to view and modify them. You are also able to configure web filtering.

### Example

Firewall policy rules control the flow of network traffic between security zones. Firewall policy rules control traffic flow based on source and destination security zones and network protocol.

```
Would you like to modify firewall policy rules? <Y,[N]>:y
```

```
The current state of firewall rules is as follows:
```

| ID | Action | Source | Destination | Service           | E |
|----|--------|--------|-------------|-------------------|---|
| 1  | permit | LAN    | WAN         | ANY               | X |
| 2  | permit | WAN    | this-device | vpn-protocols     | X |
| 3  | permit | LAN    | this-device | management        | X |
| 4  | permit | LAN    | this-device | network-protocols | X |

Key: (E)nabled

Modifying the firewall rules via this wizard resets the rules to a default state and allows you to configure basic policies for Internet access, web filtering, and device management.

```
Do you want to continue? <Y,[N]>:y
```

```
Would you like default policies allowing all internal security
zones access to the Internet? <Y,[N]>:y
```

You may now choose to enable the web filtering service. Note that access to this service requires a subscription.

```
Would you like to enable web filtering (license required) and
set up firewall rules for all internal security zones? <Y,[N]>:y
```

```
Please choose a web filtering server. For best performance,
select the server location that is closest to you. Available
locations are:
```

```
# Location
1 North America (us.surfcpa.com)
2 Europe 1      (uk1.surfcpa.com)
3 Europe 2      (uk2.surfcpa.com)
4 Asia          (asia.surfcpa.com)
```

```
Enter web filtering server selection []: 3
```

```
Would you like to allow management of the device from the
external security zone (inband management)? <Y,[N]>:y
```

```
Would you like to enable DHCP server on internal security zones
<Y,[N]>:y
```

## Enabling SMS Configuration

The SMS Configuration dialog enables or disables configuration of the device by a Security Management System (SMS). If you enable this feature, you will be prompted to enter the IP address of the SMS device that you want to manage the X family device. The X family device will initiate a call to the SMS to begin the acquisition of the configuration files.



**Note:** The SMS must be correctly configured to enable remote deployment to the device. For detailed information about the SMS and remote deployment, see “X Family Remote Deployment” in the SMS User’s Guide.

By default, the external virtual interface on the X family device uses DHCP to acquire a dynamic IP address from a DHCP Server. You do not need to make any changes to the default setting when you enable SMS configuration. Additional configuration will be required if you use other external IP address options such as static, PPPoE, PPTP, or L2TP. The following example assumes that the X family device is using the default external virtual interface settings.

### Example

```
SMS-based configuration allows the device to retrieve the
configuration for a secure management VPN to the SMS system.
This ensures that the device can be managed securely from the
SMS
```

```
Would you like to enable SMS-based configuration? <Y,[N]>:y
```

```
Enter Primary Security Management System IP Address []:
10.24.54.210
```

```
Do you have a redundant SMS server? <Y,[N]>: n
```

```
Primary SMS IP address: 10.24.54.210
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

When the SMS is on a different site than the device, a potential misconfiguration in the SMS may result in the loss of remote management access to the device. To protect against this you can enable a firewall rule to allow SSH and HTTPS access into the device from the WAN security zone and the internet. This rule will only be enabled after the SMS has timed out trying to acquire the device. During the time the firewall rule is enabled, management access to the device will be available to any IP address on the internet providing the correct username and password.

Would you like to enable WAN access on SMS configuration failure? <Y,[N]>: N

## Web, CLI, and SNMP Server Options

The Web, CLI, and SNMP Server Options dialog turns the X family device servers on and off. You should always use the secure Web and CLI servers (HTTPS and SSH) when conducting normal operations. You should only use the non-secure (HTTP) servers for troubleshooting if you cannot get the secure alternatives running for some reason.



**Note:** You do not need to run any servers if you want to control the X family device only through the serial port, but you will be unable to manage filters without servers. You can turn off all servers by using the following commands:

- `conf t server no http`
- `conf t server no https`
- `conf t server no ssh`
- `conf t sms no v2`

You must reboot the device for changes to HTTP or HTTPS to take effect.

## Secure and Non-Secure Operation

You can enable the secure and non-secure servers for the CLI (SSH and HTTP). You cannot enable both the secure and non-secure servers for the Web. This is to prevent inadvertent security lapses within your network security infrastructure. In practical terms, this means that if you enable the HTTPS server, the HTTP server is disabled.

## SMS Operation

The HTTPS server is required for SMS management. The implication of this is that if you will be using the SMS to manage the devices, you cannot run the non-secure HTTP server.

## Default Server Settings

The default settings of the Web, CLI, and SNMP servers are:

**Table 1–5: Default Web, CLI, and SNMP Server Options**

| Name  | Default Setting | Required By             | Reboot Required |
|-------|-----------------|-------------------------|-----------------|
| SSH   | ON              | secure CLI over network | no              |
| HTTPS | ON              | SMS, secure LSM         | yes             |
| HTTP  | OFF             | non-secure LSM          | yes             |
| SNMP  | ON              | SMS, NMS                | yes             |



**Note:** You can use the CLI `reboot` command to reboot the X family device if you modify settings for which a reboot is required.

### SSH Server

The SSH Server enables encrypted terminal communications. The SSH server must be enabled to establish a secure CLI session over your network.

### HTTPS Server

The HTTPS web server enables encrypted file transfers over the network. The HTTPS server must be enabled to use SMS management. You can also run the LSM using the HTTPS server.

### HTTP Server

You can enable the HTTP server to run non-secure LSM sessions on your network.



**CAUTION:** HTTP is not a secure service. If you enable HTTP, you endanger the security of the X family device. Use HTTPS instead of HTTP for normal operations.

### SNMP Server

The SNMP Server provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). The SNMP server must be enabled to use SMS management or to allow NMS access.

### Example

The Server Options dialog follows:

```
Server options allow you to enable or disable each of the
following servers: SSH, , HTTPS, HTTP, and SNMP.
Would you like to modify the server options? <Y, [N]>: y

Enable the SSH server? [Yes]:y
Enable the HTTPS server ('No' disables SMS access)? [Yes]:y
Enable the HTTP server? [No]:n
```

```
Enable the SNMP agent ('No' disables SMS and NMS access)?  
[Yes]:y  
  
SSH: Yes  
HTTPS: Yes  
HTTP: No  
SNMP: Yes  
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: e
```

## NMS Settings

The NMS Options dialog configures the Network Monitoring System (NMS) settings available for the device. This feature enables monitoring of the device by an NMS, such as HP OpenView.

### Example

The NMS Options dialog follows:

```
A Network Management System (NMS) such as HP OpenView (TM) can  
be used to monitor and receive traps from your device.  
  
Would you like to configure a Network Management System?  
<Y,[N]>: y
```

## Restrict SMS

This option configures the device to accept management only from an SMS at a specified IP address.

### Example

The Restricted SMS Access dialog follows:

```
SMS sourced configuration allows the device to retrieve the configuration for a  
secure management VPN to the SMS system. This will ensure that the device can be  
managed securely from the SMS  
Would you like to enable SMS based configuration? <Y,[N]>:n
```

## Additional Configuration

After you have run the initial setup wizard through the Command Line Interface via a serial terminal, you can further configure the device. These subsequent setup options include the following:

- [“Changing Network Deployment Configuration” on page 16](#)
- [“Ethernet Port Settings” on page 17](#)
- [“Default Email Contact Information” on page 18](#)

## Changing Network Deployment Configuration

Use the **setup x-series** command to change network deployment options. Depending on the options that you select, you may also be required to change your virtual interface configuration.

## Example

In this example, the X family device was originally configured in Routed mode, as described in [“Network Deployment Configuration” on page 9](#). In changing to NAT mode, an external virtual interface must also be configured, and you are prompted to do so after selecting NAT mode. The default IP addresses are accepted, and no additional configurations are made.

```

device1# setup x-series

Would you like to modify the network deployment mode? <Y,[N]>:y

Please choose a network deployment option:

    1) Routed mode
    2) NAT mode
    3) Transparent (layer 2) mode

Please Select []: 2

You must now configure the external interface.

Mode (static, dhcp, pppoe, pptp, l2tp) [static]: dhcp

Your selected deployment mode requires an internal interface in
order to function correctly. Would you like to create one now?
<Y,[N]>:y

IP Address [192.168.1.254]:
Mask [255.255.255.0]:

Would you like to modify virtual interfaces? <Y,[N]>:n
Would you like to modify security zones? <Y,[N]>:n
Would you like to modify security zone to virtual interface
mapping? <Y,[N]>:n
Would you like to modify firewall policy rules? <Y,[N]>:n
Would you like to enable SMS based configuration? <Y,[N]>:n

```

## Ethernet Port Settings

The Ethernet port configuration dialog does not run in the Out-of-the-Box Setup Wizard. You can only access the Ethernet Port Setup by using the `setup` command in the CLI.



**Tip:** You can configure Ethernet ports individually using the `conf t interface ethernet` command.



**CAUTION:** When you configure an Ethernet port using the command line interface, the port will be shut down. Use the `conf t int ethernet <slot> <port> no shutdown` command to restart the port.

## Ethernet Port Options

The Ethernet Port Options dialog sets individual port values for the Ethernet interface.

### Line Speed

The line speed setting for port. A valid entry will meet the following criterion:

- either 10 or 100

### Duplex Setting

The duplex setting for the port. A valid entry must be one of the following:

- copper - full or half

### Auto Negotiation

The auto negotiation setting determines whether the port will negotiate its speed based on the connection it can make. A valid entry must be one of the following:

- on
- off

### Example

An excerpt of the Ethernet Port Options dialog follows:

```
device18# setup eth

Configure slot 3 (Ethernet Ports)? <Y,[N]>:y
Configure port 1 (Ethernet Port)? <Y,[N]>:y
This port is currently enabled, would you like to disable it?
<Y,[N]>:n
Please enter values for the following options
    Line speed [100]:
    Duplex setting [Full]:
    Auto negotiation [On]:

The settings entered for slot 3, port 1 are as follows:
    Line speed: 100
    Duplex setting: Full
    Auto negotiation: On

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
Configure port 2 (Ethernet Port)? <Y, [N] >:
```



**CAUTION:** When you configure a Ethernet port using the command line interface, the port will be shut down. Use the `conf t int ethernet <slot> <port> no shutdown` command to restart the port.

## Default Email Contact Information

The Default Alert options dialog does not run in the Out-of-the-Box Setup Wizard. You can only access the Management Port Routing options by using the `setup` command in the CLI.

These options enable you to establish the default sender and recipient for filter alert e-mails.

**TO email address**

The TO email address is the email address to which alert notifications will be sent. A valid entry must meet the following criteria:

- must be less than 129 characters long
- must be a valid email address. For example: johndoe@mycompany.com

**FROM email address**

The FROM email address is the address that alert notifications will contain in the from field. A valid entry will meet the following criteria:

- must be less than 129 characters long
- must be a valid email account name on the SMTP server
- must be a valid email address on the SMTP server

**Domain**

The Domain Name is the domain name of the SMTP server. A valid entry will meet the following criteria:

- must be a valid domain name with a DNS entry on the network the device is located on
- must be the domain name where the SMTP server is located

**Email Server IP address**

The email Server IP address should be the address where the SMTP server is located. A valid entry will meet the following criterion:

- must be a valid IP address for an SMTP server

**Period**

The Period is the aggregation period for email alerts. The first time a filter that calls for email notification is triggered, the device sends an email notification to the target named in the filter. At the same time, the aggregation timer starts. The device counts additional filter triggers, but does not email another notification until it sends a count of all filter triggers that occurred during that period. The timer continues to count and send notifications at the end of each period. A valid entry will meet the following criterion:

- an integer between 1 and 10,080 representing minutes between notifications

**Example**

The Default Email Contacts Dialog follows:

```
Would you like to modify the default Email contact? <Y,[N]>:y
Enter TO: email address (128 max. characters)
Must be a full email address (e.g., recipient@company.com) []:
employee@company.com
Enter FROM: email address (128 max. characters)
Must be a full email address (e.g., sender@company.com) []:
acme@company.com
Enter FROM: Domain Name (128 max. characters, e.g., company.com)
[]: company.com
```

```
Enter email server IP address []: 1.2.3.4
Enter period (in minutes) that email should be sent (1 - 10080)
[1]: 5

      To: employee@company.com
      From: acme@company.com
      Domain: company.com
      Email Server: 1.2.3.4
      Period (minutes): 5
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

## After the Setup Wizard

After you have completed the setup wizard, if you have changed from the HTTPS to HTTP server or SNMP, you must reboot. You can accomplish this by issuing the `reboot` command from the CLI. After the device reboots, you can use the Local Security Manager graphical user interface (GUI) to perform monitoring and configuration tasks.



**Note:** The X family device allows for 10 web client connections, 10 SSH (for CLI) connections, and 1 console connection at any given time.

# 2 Command Reference

*Descriptions and usage of CLI commands.*

## Overview

The following tables list the CLI commands by functionality, grouped according to the corresponding LSM pages. Some CLI commands do not have corresponding functions in the LSM, and are listed in Table 2–9 on page 27.

**Table 2–1: LSM Home Page**

| LSM Screen    | CLI Command  | Page                |
|---------------|--------------|---------------------|
| LSM Home Page | reboot       | <a href="#">85</a>  |
|               | show log     | <a href="#">98</a>  |
|               | show version | <a href="#">117</a> |
|               | logout       | <a href="#">83</a>  |

**Table 2–2: IPS Commands**

| LSM Screen                           | CLI Command                 | Page               |
|--------------------------------------|-----------------------------|--------------------|
| Security Profiles: Category Settings | conf t category-settings    | <a href="#">38</a> |
|                                      | show conf category-settings | <a href="#">88</a> |
| Traffic Threshold                    | conf t filter               | <a href="#">44</a> |
|                                      | show conf filter            | <a href="#">89</a> |
|                                      | show filter                 | <a href="#">94</a> |

**Table 2–2: IPS Commands (Continued)**

| LSM Screen   | CLI Command                  | Page                |
|--------------|------------------------------|---------------------|
| Action Sets  | conf t notify-contact        | <a href="#">58</a>  |
|              | conf t default-alert-sink    | <a href="#">40</a>  |
|              | show action-sets             | <a href="#">87</a>  |
|              | show conf default-alert-sink | <a href="#">89</a>  |
|              | show conf notify-contacts    | <a href="#">91</a>  |
|              | show default-alert-sink      | <a href="#">93</a>  |
| IPS Services | conf t port                  | <a href="#">59</a>  |
|              | show conf port               | <a href="#">91</a>  |
| Preferences  | conf t protection-settings   | <a href="#">60</a>  |
|              | conf t tse                   | <a href="#">67</a>  |
|              | show conf tse                | <a href="#">92</a>  |
|              | show protection-settings     | <a href="#">111</a> |

**Table 2–3: Firewall Commands**

| Firewall Rules  | conf t firewall rule               | <a href="#">45</a> |
|-----------------|------------------------------------|--------------------|
|                 | show conf firewall rule            | <a href="#">89</a> |
|                 | show firewall rules                | <a href="#">94</a> |
| Services        | conf t firewall service            | <a href="#">48</a> |
|                 | show conf firewall service         | <a href="#">90</a> |
|                 | show conf firewall service-group   | <a href="#">48</a> |
|                 | conf t firewall alg                | <a href="#">45</a> |
|                 | conf t firewall service-group      | <a href="#">48</a> |
|                 | show conf firewall alg             | <a href="#">90</a> |
| Schedules       | conf t firewall schedule           | <a href="#">47</a> |
|                 | show conf firewall schedule        | <a href="#">90</a> |
| Virtual Servers | conf t firewall virtual-servers    | <a href="#">49</a> |
|                 | show conf firewall virtual-servers | <a href="#">90</a> |

**Table 2–3: Firewall Commands (Continued)**

| Web Filtering | conf t web-filtering                   | <a href="#">78</a> |
|---------------|----------------------------------------|--------------------|
|               | show conf web-filtering                | <a href="#">92</a> |
|               | show conf web-filtering filter-service | <a href="#">93</a> |
|               | show conf web-filtering manual-filter  | <a href="#">93</a> |

**Table 2–4: VPN Commands**

| IPSec Status  | conf t vpn ipsec       | <a href="#">74</a>  |
|---------------|------------------------|---------------------|
|               | show conf vpn ipsec    | <a href="#">92</a>  |
|               | show conf vpn ipsec sa | <a href="#">92</a>  |
|               | show vpn ipsec         | <a href="#">117</a> |
|               | conf t vpn debug       | <a href="#">71</a>  |
| IKE Proposals | conf t vpn ike         | <a href="#">71</a>  |
|               | show conf vpn ike      | <a href="#">92</a>  |
| L2TP Status   | conf t vpn l2tp        | <a href="#">76</a>  |
|               | show conf vpn l2tp     | <a href="#">117</a> |
|               | show vpn l2tp          | <a href="#">92</a>  |
| PPTP Status   | conf t vpn pptp        | <a href="#">77</a>  |
|               | show conf vpn pptp     | <a href="#">92</a>  |
|               | show vpn pptp          | <a href="#">117</a> |

**Table 2–5: Event Commands**

| Logs   | clear log               | <a href="#">31</a>  |
|--------|-------------------------|---------------------|
|        | conf t log audit select | <a href="#">56</a>  |
|        | show conf log           | <a href="#">91</a>  |
|        | show log                | <a href="#">98</a>  |
|        | show np                 | <a href="#">101</a> |
|        | show policy counters    | <a href="#">111</a> |
| Health | show health             | <a href="#">95</a>  |

**Table 2–5: Event Commands (Continued)**

| Reports | show tse                     | <a href="#">116</a> |
|---------|------------------------------|---------------------|
|         | show firewall monitor        | <a href="#">94</a>  |
|         | show firewall rules counters | <a href="#">94</a>  |

**Table 2–6: System Commands**

| Update                           | boot                        | <a href="#">29</a>  |
|----------------------------------|-----------------------------|---------------------|
|                                  | conf t autodv               | <a href="#">37</a>  |
|                                  | show autodv                 | <a href="#">87</a>  |
|                                  | show conf autodv            | <a href="#">89</a>  |
|                                  | snapshot                    | <a href="#">118</a> |
| Configuration: Time Options      | conf t clock                | <a href="#">38</a>  |
|                                  | show clock                  | <a href="#">88</a>  |
|                                  | conf t ntp                  | <a href="#">58</a>  |
|                                  | show ntp                    | <a href="#">111</a> |
|                                  | show timezones              | <a href="#">115</a> |
| Configuration: SMS/NMS           | conf t sms                  | <a href="#">66</a>  |
|                                  | conf t nms                  | <a href="#">58</a>  |
|                                  | show conf sms               | <a href="#">92</a>  |
|                                  | show conf nms               | <a href="#">91</a>  |
|                                  | show sms                    | <a href="#">115</a> |
| Configuration: High Availability | high-availability           | <a href="#">82</a>  |
|                                  | conf t high-availability    | <a href="#">49</a>  |
|                                  | show conf high-availability | <a href="#">90</a>  |
|                                  | show high-availability      | <a href="#">96</a>  |
| Configuration: Thresholds        | conf t monitor threshold    | <a href="#">57</a>  |
| Configuration: Email Server      | conf t default-alert-sink   | <a href="#">40</a>  |
|                                  | conf t email-rate-limit     | <a href="#">43</a>  |
|                                  | show conf email-rate-limit  | <a href="#">89</a>  |
|                                  | show default-alert-sink     | <a href="#">93</a>  |

**Table 2–6: System Commands (Continued)**

|                               | show conf default-alert-sink | <a href="#">89</a>  |
|-------------------------------|------------------------------|---------------------|
| Configuration: Syslog Servers | conf t remote-syslog         | <a href="#">62</a>  |
|                               | show conf remote-syslog      | <a href="#">91</a>  |
| Configuration: Setup Wizard   | setup                        | <a href="#">86</a>  |
|                               | show conf host               | <a href="#">64</a>  |
|                               | conf t server                | <a href="#">64</a>  |
|                               | show conf server             | <a href="#">92</a>  |
|                               | show chassis                 | <a href="#">87</a>  |
|                               | conf t clock                 | <a href="#">38</a>  |
|                               | conf t ntp                   | <a href="#">58</a>  |
|                               | show clock                   | <a href="#">88</a>  |
|                               | show timezones               | <a href="#">115</a> |
|                               | conf t interface virtual     | <a href="#">51</a>  |
|                               | show conf interface virtual  | <a href="#">91</a>  |
|                               | conf t zone                  | <a href="#">80</a>  |
|                               | show conf zone               | <a href="#">93</a>  |
|                               | conf t dns                   | <a href="#">43</a>  |
|                               | show conf dns                | <a href="#">89</a>  |
|                               | conf t interface ethernet    | <a href="#">50</a>  |
|                               | show conf interface ethernet | <a href="#">90</a>  |
|                               | conf t default-alert-sink    | <a href="#">40</a>  |
|                               | show conf default-alert-sink | <a href="#">89</a>  |

**Table 2–7: Network Commands**

| Configuration: Network Ports  | conf t int ethernet    | <a href="#">50</a> |
|-------------------------------|------------------------|--------------------|
|                               | show conf int ethernet | <a href="#">90</a> |
|                               | show int ethernet      | <a href="#">96</a> |
| Configuration: Security Zones | conf t zone            | <a href="#">80</a> |
|                               | show conf zone         | <a href="#">93</a> |

**Table 2–7: Network Commands (Continued)**

| Configuration: IP Interfaces     | conf t interface virtual    | <a href="#">51</a>  |
|----------------------------------|-----------------------------|---------------------|
|                                  | show conf interface virtual | <a href="#">91</a>  |
|                                  | show interface virtual      | <a href="#">96</a>  |
| Configuration: IP Address Groups | conf t address-group        | <a href="#">35</a>  |
|                                  | show conf address-group     | <a href="#">89</a>  |
| Configuration: DNS               | conf t dns                  | <a href="#">43</a>  |
|                                  | show conf dns               | <a href="#">89</a>  |
| Configuration: Default Gateway   | conf t default-gateway      | <a href="#">41</a>  |
|                                  | show conf default-gateway   | <a href="#">87</a>  |
| Routing                          | conf t routing              | <a href="#">63</a>  |
|                                  | show conf routing           | <a href="#">91</a>  |
|                                  | show conf routing multicast | <a href="#">91</a>  |
|                                  | show routing                | <a href="#">113</a> |
| DHCP Server                      | conf t dhcp-server          | <a href="#">41</a>  |
|                                  | show conf dhcp-server       | <a href="#">89</a>  |
|                                  | show dhcp-server            | <a href="#">93</a>  |
| Tools                            | ping                        | <a href="#">84</a>  |
|                                  | tracert                     | <a href="#">118</a> |
|                                  | traffic-capture             | <a href="#">119</a> |

**Table 2–8: Authentication Commands**

| User List | conf t local-user | <a href="#">55</a>  |
|-----------|-------------------|---------------------|
|           | conf t user       | <a href="#">67</a>  |
|           | show conf user    | <a href="#">92</a>  |
|           | show local-user   | <a href="#">98</a>  |
|           | show user         | <a href="#">116</a> |
|           | who               | <a href="#">121</a> |
|           | whoami            | <a href="#">122</a> |

**Table 2–8: Authentication Commands (Continued)**

| Privilege Groups | conf t authentication privilege-groups   | <a href="#">36</a> |
|------------------|------------------------------------------|--------------------|
|                  | show conf authentication privilege-group | <a href="#">89</a> |
| RADIUS           | conf t authentication radius             | <a href="#">36</a> |
|                  | show conf authentication radius          | <a href="#">89</a> |
| Preferences      | conf t user options                      | <a href="#">68</a> |

**Table 2–9: CLI Commands**

| CLI history commands    | !                 | <a href="#">28</a>  |
|-------------------------|-------------------|---------------------|
|                         | history           | <a href="#">83</a>  |
| CLI management commands | alias             | <a href="#">28</a>  |
|                         | bugreport         | <a href="#">30</a>  |
|                         | cls               | <a href="#">33</a>  |
|                         | conf t session    | <a href="#">65</a>  |
|                         | show conf session | <a href="#">92</a>  |
|                         | show session      | <a href="#">114</a> |
|                         | exit              | <a href="#">81</a>  |
|                         | help              | <a href="#">82</a>  |
|                         | logout            | <a href="#">83</a>  |
|                         | quit              | <a href="#">85</a>  |
|                         | reboot            | <a href="#">85</a>  |
|                         | setup             | <a href="#">86</a>  |
|                         | show version      | <a href="#">117</a> |
|                         | tree              | <a href="#">120</a> |

!

access: global; all

The **!** command executes a command in the [history](#) buffer. Use **!!** to repeat the previous command executed.

---

! #

indicates an item number in the [history](#) buffer. Use **! #** to execute command **#** in the history buffer. See [“execute command <number> from history buffer” on page 83](#) for an example.

### alias

access: global; all

The **alias** command lists defines abbreviated commands. The command accepts an alias and the string that the alias will represent.

---

alias-name

The character string that you will type instead of the full command string. It must be a unique combination of letters, numbers, and hyphens or underscores.

---

"command-string"

A text string that is either a valid CLI command or part of a command. If the string contains blanks, you must enclose the string in quotes.

### Using the alias command

*create a new  
alias*

Enter the **alias** command with an alias name and a command string enclosed in quotes.

```
hostname# alias eth "ethernet"
```

*show aliases*

Enter the **alias** command without any parameters to show a list of currently defined aliases.

```
hostname# alias
eth          ethernet
```

*delete an alias* Enter the **alias** command with an existing alias and no other parameters to delete that alias.

```
hostname# alias eth
```



**Note:** You cannot define an alias for an alias. Every alias must refer directly to a valid CLI command, or to valid command input.

## boot

access: local; super, admin

The **boot** command lists, rolls back to, and removes prior boot images on the device.



**Note:** The device can store several software images. A minimum of one saved image is required for rollback purposes.

---

### list-image

shows a list of all available boot images.

---

### remove-image version

removes a boot image from the device's hard disk. This command is disabled when the SMS manages the device.



**CAUTION:** When you remove a boot image, the image is permanently erased from the device's hard drive. The only way to reinstall that image is to perform the update process using the Local Security Manager.

---

### rollback

rolls the boot image back to the next most current valid boot image. This command can be used to revert the operating system to a previous version. For example, if you install the wrong update image to the device, you can use the **boot rollback** command to restore the previous image. This command is disabled when the SMS manages the device.



**CAUTION:** When you perform a rollback, you permanently erase the most current boot image on the device's hard drive. The only way to replace this image is to perform the update process through the Local Security Manager.

---

### Using the boot command

*view available  
boot images*

Enter **boot list-image** to list all available boot images.

```
hostname# boot list-image  
image1 image2 image3
```

*remove a boot  
image from  
the device's  
hard disk*

Enter **boot remove-image** *image-name* to remove a boot image from the device.

```
hostname# boot remove-image image2
```

*roll back to  
the next most  
current image*

Enter **boot rollback** to roll back to a previous boot image.

```
hostname# boot rollback
```

---

### bugreport

access: local, super, admin, operator

The **bugreport** command polls the device for statistics and other relevant information and sends the information as a clear-text e-mail message to the specified e-mail address. You should only execute this command when requested by support personnel.

The command may take a minute to execute. The default e-mail options must be configured for the e-mail transfer to succeed. This can be accomplished using the **setup email-default** command.



**CAUTION:** Since this information is transferred via e-mail, it is transferred on an unsecured channel in clear text. While we do not consider the system snapshot information to constitute a security risk, you may choose to report system problems by other methods. If so, please contact the Technical Assistance Center (TAC) to make other arrangements.

---

#### email-address

the email address of your designated bug report recipient. This must be a valid email user name on the email notification server.

---

#### "description"

a short description (in double quotes) of the bug that the user is experiencing.

## clear

access: global; super, admin

The **clear** command resets logs or hardware interfaces. The command requires one of the following subcommands.

---

### arp-cache

clears dynamic entries from the Address Resolution Protocol (ARP) cache. ARP is an internet protocol used to map an IP address to a MAC address.

---

### connection-table blocks

clears all connection table block entries.

---

### counter interface

clears interface counters. This command is disabled when the SMS manages the device.

#### ethernet

clears Ethernet interface counters. When used without slot and port information, it clears the counters for all Ethernet interfaces on the device.

#### mgmtEthernet

clears the counters for the Management Ethernet port on the device.

---

### counter policy

clears all policy counters. This command is disabled when the SMS manages the device.

---

### interface

clears the interface. When used without parameters, the command resets all interfaces on the device. This command is disabled when the SMS manages the device.

#### ethernet [slot] [port]

clears the Ethernet interface. When used without parameters, the command clears all Ethernet ports.

##### slot

clears all Ethernet ports in the blade that sits in *slot*.

##### port

clears the numbered port.

---

### **log [alert | audit | block | firewallblock | firewallsession | packet-trace | system | vpn]**

clears the specified log or logs. When used without parameters, the command erases all entries in all logs. This command is disabled when the SMS manages the device.



**Note:** When admin-level users issue the **clear log** command without parameters, the audit log is not cleared. Only super-user-level users can clear the audit log.

---

### **np [rule-stats | softlinx]**

clears the statistical information related to either rules or the Softlinx.

---

### **ramdisk stats**

clears the statistical information related to the RAM disk.

---

### **rate-limit streams**

clears rate limited streams from the data table.

---

## **Using the clear command**

*clear all  
ethernet  
counters*

Enter **clear counter interface ethernet** without the slot or port parameters to clear the counters for all Ethernet ports in all slots.

```
hostname# clear count int ethernet
```

*clear ethernet  
counters of a  
specific slot*

Enter **clear counter interface ethernet slot-number** without the port parameter to clear the counters for all Ethernet ports in a slot.

```
hostname# clear count int ethernet 7
```

*clear ethernet  
counter for a  
specific port*

Enter **clear counter interface ethernet slot-number port-number** to clear the counters for a specific Ethernet port.

```
hostname# clear count int ethernet 7 2
```

*clear all  
Management  
Ethernet  
counters*

Enter **clear counter interface mgmtEthernet** to clear all Management Ethernet counters.

```
hostname# clear count int mgmtethernet
```

*reset all  
interfaces*

Enter the **clear interface** command without any other parameters to reset the chassis. You will be asked to confirm this command.

```
hostname# clear interface
```

*reset the card  
in slot n*

Enter the **clear interface** command and a slot number to reset the interface card in the specified slot.

```
hostname# clear interface 2
```

*reset port x on  
the interface  
card in slot n*

Enter the **clear interface** command, a slot number, and a port number to reset the specified port.

```
hostname# clear interface 2 1
```

*erase all  
entries in all  
logs*

Enter the **clear log** command without any parameters to erase all entries in all logs.

```
hostname# clear log
Are you sure you want to clear out ALL logs? <Y,[N]>:Y
```

## cls

access: global; all

The **cls** command clears the screen.

### Using the CLS command

*clear the  
screen*

Enter the **cls** command to clear the screen.

```
hostname# cls
```

## configure

access: local; super, admin, operator can configure own session and change own password; clock - super; ntp - super

The **configure** commands configure X family software and hardware settings.

### terminal

The **configure terminal** commands change settings for many features of the device.



**Tip:** You can use the abbreviated form: **conf t**. You can also use a predefined alias: **cft**.



**Note:** When you enter 8 asterisks (\*\*\*\*\*) as a password in a **configure terminal** command, the password will be set to the default value, which is **password**.

---

### **conf t action-set** action-set-name threshold threshold-period

The configure terminal action-set command configures new or existing action sets. The following subcommands determine the action that each named action set takes.

#### **allowed-dest** [add | remove]

adds or removes a quarantine allowed destination.

#### **apply-only** [add | remove]

adds or removes a CIDR from the quarantine apply-only list.

#### **block**

creates or modifies an action set that blocks traffic.

#### **quarantine**

creates or modifies an action set that quarantines blocked traffic.

#### **reset-both**

creates or modifies an action set that performs a TCP reset on both the source and destination of blocked traffic.

#### **reset-destination**

creates or modifies an action set that performs a TCP reset on the destination of blocked traffic.

#### **reset-source**

creates or modifies an action set that performs a TCP reset on the source of blocked traffic.

#### **delete**

deletes the named action set.

#### **non-web-block**

blocks non-web requests from quarantined hosts. Use **non-web-block no** to permit non-web requests.

#### **notify-contact** [add | remove]

adds or removes a notification contact from an action set

#### **packet-trace**

enables and sets packet trace settings. You can enter a priority (high, medium, or low) and the number of bytes to capture (64-1600).

#### **permit**

creates or modifies an action set that permits traffic.

#### **rate-limit** rate

creates or modifies an action set that rate-limits. Enter the desired rate in Kpbs.

**rename**

renames the action set.

**web-block**

blocks web requests from quarantined hosts.

**web-page**

creates an internal web page to display web requests from a quarantined host.

**web-redirect url**

redirects web requests from a quarantined host to the URL that you specify.

**whitelist [add | remove]**

adds or removes a CIDR from a quarantine whitelist. Whitelisted CIDRs are always permitted.

---

**conf t address-groups**

The **configure terminal address-groups** commands configure IP address groups for the devices.

**add-entry name < host ip | subnet ip netmask mask | range ip1 ip2 >**

adds an IP subnet, IP host, or IP range to an IP address group.

**remove name**

deletes an IP address group.

**remove-entry name < host ip | subnet ip netmask mask | range ip1 ip2 >**

removes an IP subnet, IP host, or IP range from an IP address group.

**update name < host ip | subnet ip netmask mask | range ip1 ip2 >**

updates the settings of an existing IP address-group or creates a new IP address-group.

---

**Using the conf t address-group command***update an IP address group*

Use **configure terminal address-group update** to update an IP address group. In this example, the group “test” is set as the single host 1.2.3.4”

```
hostname# conf t address-group update test host 1.2.3.4
```

*add an IP subnet to an IP address group*

Use **configure terminal address-group add-entry** to add an entry to an IP address group. In this example, the 192.168.1.0/24 subnet is added to the “test” group:

```
hostname# conf t address-group add-entry test subnet 192.168.1.0
netmask 255.255.255.0
```

*delete an IP subnet from an IP address group*

Use **configure terminal address-group remove-entry** to delete an entry from an IP address group. In this example, the 192.168.1.0/24 subnet is deleted from the “test” group:

```
hostname# conf t address-group remove-entry test subnet 192.168.1.0
netmask 255.255.255.0
```

### *delete an IP address group*

Use **configure terminal address-group remove** to delete an IP address group. In this example, the “test” group is deleted:

```
hostname# conf t address-group remove test
```

---

### **conf t authentication**

The **configure terminal authentication** command configures RADIUS authentication and privilege groups on the device.

#### **privilege-groups remove** name

deletes a privilege group.

#### **privilege-groups update** name [web-filtering-bypass] [firewall-authentication] [vpn-client-access]

adds privileges to the named privilege group. These privileges will be assigned to users that authenticate either via RADIUS or via the local database.

#### **radius**

controls RADIUS authentication.

#### **default-privilege-group** priv-group

defines a privilege group for a user currently unassigned to a privilege group on the RADIUS server.

#### **disable**

disables RADIUS authentication.

#### **enable**

enables RADIUS authentication.

#### **retries** number

defines the number of times that the device will attempt to connect to the RADIUS server. If the RADIUS server does not respond after that number of retries, the device will use the local database for authentication.

#### **server** < primary | secondary > address [port port] shared-secret string auth-method < pap | chap >

configures the settings for the RADIUS server. You can configure both a primary and secondary server.

#### **server secondary none**

removes the configuration for a secondary RADIUS server.

#### **timeout** seconds

defines the time in seconds before the device will again attempt to connect to the RADIUS server (if no response was originally received from the server).

**user-authentication < enable | disable >**

enables or disables RADIUS for user authentication.

**vpn-clients < enable | disable >**

enables or disables RADIUS authentication for VPN clients.

**Using conf t authentication**

*enable  
RADIUS*

Use **configure terminal authentication radius** to enable RADIUS on the device.

```
hostname# conf t auth radius enable
```

*configure  
primary  
RADIUS  
server*

Use **configure terminal authentication radius server** to configure the IP address, port, shared secret, and authentication method of the primary RADIUS server. In this example, the primary RADIUS server is configured with the address 10.0.0.10 on port 581, with shared secret “TheSecret.” and with **pap** as the authentication method:

```
hostname# conf t auth radius server primary 10.0.0.10 port 581 shared-secret  
"TheSecret" auth-method pap
```

*create a  
privilege  
group*

Use **configure terminal authentication privilege-groups update** to create or edit a privilege group. In this example, the privilege group PrivGroup1 is granted VPN client access privilege only:

```
hostname# conf t auth priv update PrivGroup1 vpn-client-access
```

*assign users to  
a privilege  
group*

Use **configure terminal authentication radius default-privilege-group** to assign RADIUS users to the default privilege group. In this example, RADIUS users are added to the privilege group PrivGroup1:

```
hostname# conf t auth radius default-privilege-group PrivGroup1
```

**conf t autodv day day time time [-period days]**

The **configure terminal autodv** command schedules the day and time when the digital vaccine definition files are updated. **conf t no autodv** disables the digital vaccine automatic updates.

By default, that the digital vaccine update will happen weekly on the specified day. Use the **[-period days]** option to specify a different number of days between updates. For example, to schedule an update every five days, you would enter the command as follows:

```
hostname# conf t autodv 1200 -period 5
```

---

### **conf t category-settings**

The **configure terminal category-settings** command enables and disables filter categories. The command also allows you to assign a specific action set to each category. The following categories can be configured:

- exploits
- identity-theft
- im
- network-equipment
- p2p
- reconnaissance
- security-policy
- spyware
- streaming-media
- traffic-normal
- virus
- vulnerabilities

#### **category disable**

disables the filter category.

#### **category enable [-action-set action]**

enables the filter category. Use **[-action-set action]** to set a specific action set for the enabled category, such as **block** or **recommended**.

---

### **conf t clock**

The **configure terminal clock** command sets time and date functions on the device.

#### **date YYYY-MM-DD**

sets the system date.

#### **dst**

enables daylight saving time on the system clock.

#### **no dst**

disables daylight saving time.

#### **time HH:MM [:SS]**

sets the system time. The time is entered as two-digit values for hours, minutes and seconds. Valid hours entries are from 00-23. Seconds are optional.

**timezone**

sets the timezone for the device.



**Tip:** Use the [show timezones](#) command to view a list of available timezone abbreviations.



**Note:** You cannot set the time or date on the device while the NTP server is enabled. You can set the time zone.

---

**Using conf t clock**

*set the system date*

Use **configure terminal clock date** to set the system date. In this example, the date is set to March 30, 2006.

```
hostname# conf t clock date 2006-03-30
```

*set the system clock to daylight saving time*

Use **configure terminal clock dst** to enable daylight saving time on the system clock.

```
hostname# conf t clock dst
```

*turn daylight saving time off*

Use **configure terminal clock no dst** to disable daylight saving time.

```
hostname# conf t clock no dst
```

*set the system time*

Use **configure terminal clock** to set the system time. In this example, the system time is set to 3:30 PM:

```
hostname# # conf t clock time 15:30:00
```

*set the system timezone*

Use **configure terminal clock timezone** to set the system timezone. In this example, the system timezone is set to Central Standard Time (CST):

```
hostname# conf t clock timezone CST
```

---

**conf t ddos**

The configure terminal ddos command defines the settings for managing Distributed Denial of Service attacks.

**connection-flood**

configures the settings for connection flood attacks.

### **aggregate-alerts**

enables aggregation of connection flood alerts. Use **no aggregate-alerts** to disable alert aggregation.

### **cps**

configures the settings to generate alerts on the number of connections per second.

### **aggregate-alerts**

enables aggregation of alerts. Use **no aggregate-alerts** to disable alert aggregation.

---

### **conf t default-alert-sink**

The **configure terminal default-alert-sink** command defines the default email recipient of traffic-triggered alerts. **no default-alert-sink** disables the sending of alert emails.

#### **domain** domain-name

defines the domain name of the email notification server.

#### **from** email-address

defines the email address of the device. This must be a valid email user name on the email notification server.

#### **period** minutes

defines the default period of time in which the device accumulates notifications before sending an aggregate notification email

#### **server** ip

defines the IP address of the email notification server.

#### **to** email-address

defines the email recipient of traffic-triggered notifications. This must be a valid email address.

---

### **Using conf t default-alert-sink**

*set default  
notification  
recipient*

Use **configure t default-alert-sink to** set the default email notification recipient.

```
hostname# conf t default-a to kwalker@mycompany.com
```

*set default  
notification  
sender*

Use **configure terminal default-alert-sink from** to set the default email notification sender.

```
hostname# conf t default-a from ul-corpnet3@mycompany.com
```

*set email  
notification  
server IP  
address*

Use **configure terminal default-alert-sink server** to set the email notification server's IP address. In this example, the address is defined as 101.202.33.44.

```
hostname# conf t default-a server 101.202.33.44
```

*set email  
notification  
server domain  
name*

Use **configure terminal default-alert-sink domain** to set the email notification server's domain name.

```
hostname# conf t default-a domain mycompany.com
```

---

### **conf t default-gateway ip**

The **configure terminal default-gateway** command defines a default gateway for the device. The command configures the default route which is used to direct traffic when the device has no specific route information for the destination. Normally this is the address of the ISP or upstream router attached to the external virtual interface on the WAN port. In some network topologies another internal device provides the route to the nternet; if so, this address can be a router on an internal virtual interface. **conf t no default-gateway** disables the default-gateway feature.

*set the default  
gateway*

Use **conf t default-gateway** to set the default gateway. In this example, the gateway address is defined as 111.222.33.200:

```
conf t default-g 111.222.33.200
```

---

### **conf t dhcp-server**

The **configure terminal dhcp-server** command configures the DHCP server inside the device.

**addresses < group group-name | subnet ip netmask mask | range ip1 ip2 | none >**  
configures the pool of IP addresses that are available to DHCP clients. The **none** option removes an address group which was previously configured as the DHCP server address pool source.

**bootp < enable | disable >**  
enable or disable bootp.

**disable**  
disables the DHCP server.

**dns < default | server1 ip1 [server2 ip2 [server3 ip3] ] [domain domain-name] >**  
configures DNS settings for the DHCP server.

**enable**  
enables the DHCP server.

**lease-duration mins**  
set the lease duration time in minutes.

**nbx nbx-ip**  
provides the NBX call processor address to phones that acquire their address via DHCP.

**relay < disable | broadcast | <server ip [ relay-from-vpn] | tunnel tunnel-name >**  
configures DHCP relay.

### **broadcast**

enables a central VPN DHCP relay agent that will broadcast DHCP requests received from a VPN tunnel.

### **disable**

disables DHCP relay.

### **server ip [ relay-from-vpn]**

sets the device to relay DHCP messages to a DHCP server at the IP address specified. Use the **relay-from-vpn** option to relay DHCP messages received from a VPN tunnel to the specified DHCP server.

### **tunnel tunnel-name**

sets the device to relay DHCP messages over the named VPN tunnel.

### **static-map add ip mac mac**

assigns a static IP address to the device with the specified MAC address.

### **static-map remove ip**

deletes a static mapping.

### **wins [primary server] [secondary server]**

defines a primary or secondary WINS server.

---

## Using `conf t dhcp-server`

*enable DHCP  
on the device*

Use **configure terminal dhcp-server** to enable the device's DHCP server.

```
hostname# conf t dhcp-server enable
```

*configure the  
address pool  
of the DHCP  
server*

Use **configure terminal dhcp-server addresses** to configure the IP address pool of the DHCP server. In this example, the DHCP scope is set as the address group 'dhcp':

```
hostname# conf t dhcp-server addresses group dhcp
```

*remove DHCP  
scope settings*

Use **configure terminal dhcp-server addresses none** to deconfigure the DHCP scope settings when the DHCP server is disabled.

```
hostname# conf t dhcp-server addresses none
```

*relaying  
messages*

Use **configure terminal dhcp-server relay server relay-from-vpn** to relay messages received over a VPN tunnel to DHCP server 192.168.0.200 (Central VPN Relay Agent):

```
hostname# conf t dhcp-server relay server 192.168.0.200 relay-from-vpn
Use configure terminal dhcp-server relay tunnel to relay DHCP messages over the VPN tunnel
VPNTUNNEL (Remote VPN Relay Agent):
```

```
hostname# conf t dhcp-server relay tunnel VPNTUNNEL
```

*mapping a  
static DHCP  
entry*

Use **configure terminal dhcp-server static-map add** to map a static DHCP entry for a MAC address to the IP address 1.2.3.4:

```
hostname# conf t dhcp-server static-map add 1.2.3.4 mac 00:22:44:55:66:77
```

---

### **conf t dns**

The **configure terminal dns** command manually configures the DNS server information for the device.

**domain-name** domain-name [domain-name2 [domain-name3] ]

configures up to three domain names which will be used to resolve DNS lookups.

**server** server-name [server2 server-name [server3 server-name] ]

configures up to three IP addresses of DNS servers. You can also use this command to remove DNS servers by entering 0.0.0.0 as the IP address.

**use-external-dns** < enable | disable >

enables or disables the use of a DNS configuration that is obtained through the WAN connection.

---

### **Using conf t dns**

*using  
manually  
configured  
DNS settings*

Use **configure terminal dns use-external disable** to disable the use of a DNS configuration obtained through the WAN connection:

```
hostname# conf t dns use-external disable
```

*specifying  
DNS servers*

Use **configure terminal dns server** to specify the IP addresses of DNS servers:

```
hostname# conf t dns server 10.0.0.1 10.0.0.2
```

*removing DNS  
servers*

Use **configure terminal dns server 0.0.0.0** to remove custom DNS servers:

```
hostname# conf t dns server 0.0.0.0
```

*resolving DNS  
lookups*

Use **configure terminal dns domain-name** to set the search domain for DNS lookups:

```
hostname# conf t dns domain-name mycompany.com
```

---

### **conf t email-rate-limit** number

The **configure terminal email-rate-limit** command configures the maximum number of email notifications the system will send every minute. The minimum is 1; the maximum is 35.

**conf t filter**

The **configure filter** command configures a filter's state and category for action set usage. The available states include **disabled** and **enabled**. When you configure a filter, you must know and enter the number for the filter. Only the **reset** subcommand supports "all" as an option.

**number [-profile "profile-name"] adaptive-config**

enables adaptive filtering for the filter. You must enter a filter number. You can optionally include a profile and slot for the filter's setting.

**number [-profile "profile-name"] no adaptive-config**

disables adaptive filtering for the filter. You must enter a filter number. You can optionally include a profile and slot for the filter's setting.

**number [-profile "profile-name"] add-exception source dest**

creates and adds an exception to a filter. You must include a filter number, source IP address, and destination IP address. You can optionally include a profile and slot.

**number [-profile "profile-name"] delete-copy**

deletes a copy of the filter. You must enter a filter number and profile in the command. The slot is optional.

**number [-profile "profile-name"] disable**

disables a filter given the number. You must enter a filter number. You can optionally include a profile and slot.

**number [-profile "profile-name"] enable**

enables a filter given the number. Do not use all in this command. You must enter a filter number. You can optionally include a profile and slot. The command also includes an option for action set.

**-action-set string**

specifies an action set for the filter.

**number [-profile "profile-name"] remove-exception source dest**

deletes an exception from a filter. You must include a filter number, source IP address, and destination IP address. You can optionally include a profile and slot.

**number [-profile profile-name] threshold threshold**

enables you to modify threshold settings of port scan and and host sweep filters. A scan/sweep user policy must already exist.

**number [-profile profile-name] timeout seconds**

enables you to modify timeout settings of port scan and and host sweep filters. A scan/sweep user policy must already exist.

**number [-profile "profile-name"] use-category**

sets the specified filter to use the action set of its category, removing any previous overrides. You must enter a filter number. You can optionally include a profile and slot.

**all reset**

removes all user changes to all filters' configuration and resets all filters to the default values.

**conf t firewall alg sip**

The **configure terminal firewall alg sip** command configures an application layer gateway (ALG) to permit Session Initiation Protocol (SIP) sessions.

**sdp-port-range [any | port-range]**

configures the range of port numbers that SIP sessions can use. You can enter up to 20 separate port ranges, separated by commas, such as:

8000-8500, 10000-12000, 50000-51000

The **any** parameter enables all ports to accommodate SIP sessions.

**services [any | service-name | service-group]**

configures the service name or service group that permits SIP operations. The **any** parameter enables the use of any service for the sessions.

**conf t firewall monitor < clients | services | website >**

The **configure terminal firewall monitor** command controls the collection of statistics related to firewall sessions. Data is gathered about each session when the session closes down. By default, monitors are enabled when the device starts up. Data is lost if the device is rebooted.

**reset**

immediately resets counters.

**conf t firewall rule**

The **configure terminal firewall rule** command creates and edits firewalls on the device. The firewalls control traffic passing between security zones.

**add [id] < permit | block | web-filter src-zone dst-zone service >**

adds a firewall rule. If no ID is specified, the system assigns one and displays it.

**counters-clear**

clears counters for all firewall rules.

**disable id**

disables a firewall rule.

**enable id**

enables a firewall rule.

**move id < after id | before id | to position-number >**

moves a firewall rule within the firewall table.

### **remove** id

deletes a firewall rule.

### **update** id

updates or creates a firewall with the specified ID. When a new rule is created, **permit**, **block**, or **web-filter** must be specified.

### **authentication** < disable | any | group name >

enables or disables authentication.

### **bandwidth** < disable | < rule | session > guaranteed kbps max kbps pri pri >

restricts the bandwidth.

### **comment** "description"

stores a comment for the rule.

### **counter-clear**

clears counters for the rule.

### **dst-addr** < all | group name | subnet ip netmask mask | range ip1 ip2 >

restricts destination addresses in the specified IP range.

### **logging** < enable | disable >

enables or disables logging for the rule.

### < permit | block | web-filter > src-zone dst-zone service

Required for a new rule. The variables *src-zone* and *dst-zone* can be this-device to indicate the local device.

### **position** position

the rule is placed in the specified position.

### **remote-logging** < enable | disable >

enables or disables remote logging for the rule.

### **schedule** < always | name >

schedules execution of the rule, either always or according to a named schedule.

### **src-addr** < all | group name | subnet ip netmask mask | range ip1 ip2 >

restricts source addresses in the specified IP range.

### **timeout** mins

specifies a timeout interval in minutes for the rule.

---

## Using conf t firewall rule

*create/update  
firewall rule*

Use **configure terminal firewall rule update** to create or update a firewall rule. In this example, firewall rule 10 is created as a “permit” rule for LAN to WAN and for telnet service only:

```
hostname# conf t firewall rule update 10 permit LAN WAN telnet
```

*update source  
and  
destination  
addresses*

Use **configure terminal firewall rule update** to update source and destination addresses for a firewall rule. In this example, firewall rule 10 is updated so that it restricts source addresses to the address group 'engineers', but permits any destination address:

```
hostname# conf t firewall rule update 10 src-addr group engineers dst-addr all
```

*move a  
firewall rule  
above another*

Use **configure terminal firewall move** to move a firewall rule. In this example, rule 10 is moved above rule 7:

```
hostname# conf t firewall move 10 above 7
```

*move a  
firewall rule to  
a specific  
position*

Use **configure terminal firewall move** to move a firewall rule to a specific position. In this example, rule 10 is moved to position 1 in the table:

```
hostname# conf t firewall move 10 to 1
```

---

### conf t firewall schedule

The **configure terminal firewall schedule** command limits when a firewall rule will operate.

**add-entry** schedule-name day\_letters [from time1 to time2]

add an entry to the named firewall schedule (without overwriting the other days).

**remove** schedule-name

deletes the named schedule.

**remove-entry** schedule-name day\_letters [from time1 to time2]

deletes an entry from a named schedule.

**update** schedule-name [days day\_letters [from time1 to time2] ]

creates a named firewall schedule or updated an existing schedule..



**Note:** The variable day\_letters is seven characters to represent the days and time1 and time2 are the time in 24 hours clock.

---

### Using conf t firewall schedule

*create a  
schedule*

Use **configure terminal firewall schedule** to create a schedule. In this example, a schedule named 'work' is created and scheduled for Monday through Friday from 9am to 5pm:

```
hostname# conf t firewall schedule update work days -MTWTF- from 0900 to 1700
```

In this example, a schedule named 'weekend' is created and scheduled for all day Saturday and Sunday:

```
hostname# conf t firewall schedule update weekend days S-----S
```

---

### **conf t firewall service**

Use **configure terminal firewall service** to configure the services that are used by the firewall rules.

**remove** service-name

deletes a service.

**update** service-name < **tcp** | **udp** | **icmp** | **esp** | **ah** | **gre** | **igmp** | **ipcomp** | number >  
[**port** port-number [**to** port-number] ]

creates a service or updates an existing service.

---

### **Using conf t firewall service**

*configure a  
service for an  
IP protocol*

Use **configure terminal firewall service** to create a service for an arbitrary IP protocol. In this example, a service called 'ospf' is created for IP protocol 89:

```
hostname# conf t firewall service update ospf 89
```

*create a  
service*

Use **configure terminal firewall service update** to create a service that will be used by a firewall rule. In this example, a service called 'Telnet' is created for TCP port 23:

```
hostname# conf t firewall service update Telnet tcp port 23
```

---

### **conf t firewall service-group**

The **configure terminal firewall service-group** command groups services together.

**add-service** group-name service-name

adds a service to an existing service group.

**remove** group-name

deletes a service group.

**remove-service** group-name service-name

deletes a service from a service group.

**update** group-name service-name

creates or updates a service group. You can enter multiple service names.

---

### **Using conf t firewall service-group**

*create/update  
a service  
group*

Use **configure terminal firewall service-group update** to create or update a service group. In this example, a service group called 'group1' is created, and includes Telnet and rlogin:

```
hostname# conf t firewall service-group update group1 Telnet rlogin
```

*add a service  
to a service  
group*

Use **configure terminal firewall service-group add-service** to add a service to a service group. In this example, DNS service is added to the service group named 'group1':

```
hostname# conf t firewall service-group add-service group1 dns-udp
```

---

### **conf t firewall virtual-server**

The **configure terminal firewall virtual-server** command configures a virtual server or servers that will redirect traffic to a physical server on the LAN.

**remove < all-services | service > public-ip <external | ip >**  
removes a virtual server.

**update < all-services | service > public-ip < external | ip > internal-ip ip  
[pat < disable | port >]**  
updates or creates a virtual server.

---

### **Using conf t firewall virtual-server**

*create a  
virtual server*

Use **configure terminal firewall virtual-server update** to create a virtual server. In this example, an HTTP virtual server is created and assigned to 192.168.1.1 port 90. The server accesses the external virtual interface with port address translation (PAT):

```
hostname# conf t firewall virtual-server update http public-ip external  
internal-ip 192.168.1.1 pat 90
```

*create a NAT  
mapping*

Use **configure terminal zone virtual-server update** to create a one-to-one NAT mapping. In this example, a 1-to-1 NAT mapping of 192.168.1.2 to 10.245.230.44 is created:

```
hostname# conf t firewall virtual-server update all-service public-ip 10.245.230.44  
internal-ip 192.168.1.2
```

---

### **conf t high-availability**

The **configure terminal high-availability** command configures High Availability. High Availability supports stateless failover for up to two redundant devices.

**disable**  
disables high availability on the device.

**enable**  
enables high availability on the device.

**heartbeat poll-timer wait-interval retry-count**  
sets the values for the poll timer, wait interval in milliseconds, and retry count for the heartbeat ping.

### **id** id-number

configures an ID number that will be used when a MAC address conflict occurs. Because MAC address conflicts normally do not occur, the ID number is not required. A standby device must have the same ID number as the active device for which it is on standby.

---

### **conf t interface**

The **configure terminal interface** command configures device interfaces. The command abbreviation is **conf t int**.



**Note:** When referring to an interface, use the slot number and the port number separated by a blank space. Do not use slashes, dashes, colons or any character other than a single space between the slot number and the port number when naming an interface on the command line.

### **ethernet** slot-number port-number

configures Ethernet ports on the device. The command abbreviation is **conf t int eth**.

#### **duplex < half | full >**

sets the duplex for the port to either half or full.

#### **linespeed < 10 | 100 | 1000 >**

sets the line speed for a port.

#### **negotiate**

turns auto-negotiation on. **no negotiate** turns auto-negotiation off.

#### **shutdown**

administratively closes the port. **no shutdown** restarts a port after a shutdown command or after configuration has changed.



**Note:** When you configure a Ethernet port, the port will be shut down. Use the **conf t int eth** slot port **no shutdown** command to restart the port.

---

### **Using conf t interface ethernet**

*set the line  
speed for a  
Ethernet port*

Use **configure terminal interface ethernet linespeed** to set the line speed for a Ethernet port. In this example, the line speed on slot 7, port 2 is set to 100 Mbps. The port is then restarted.

```
hostname# conf t int eth 7 2 linespeed 100
hostname# conf t int eth 7 2 no shutdown
```

*turn auto negotiation on for a Ethernet port*

Use **configure terminal interface ethernet negotiate** to enable auto negotiation for a particular Ethernet port. In this example, auto negotiation is enabled on port 8, slot 2. The port is then restarted.

```
hostname# conf t int eth 8 2 negotiate
hostname# conf t int eth 8 2 no shutdown
```

*deactivate a Ethernet port*

Use **configure terminal interface ethernet shutdown** to deactivate a Ethernet port. In this example, port 8, slot 2 is deactivated.

```
hostname# conf t int eth 8 2 shutdown
```

*reactivate a Ethernet port*

Use **configure terminal interface ethernet no shutdown** to reactivate a Ethernet port. In this example, port 8, slot 2 is reactivated.

```
hostname# conf t int eth 8 2 no shutdown
```

### settings

configures the interface to enable/disable MDI-detect when auto-negotiation is off and to set the polling interval for Ethernet port status changes.

#### detect-mdi [enable|disable]

sets the detect option for MDI as enabled or disabled.

#### mdi-mode [mdi | mdix]

indicates whether the connection is MDI or MDI-X.

#### poll-interval value

sets the polling interval for Ethernet port status changes. The value is in milliseconds.

### virtual

configures a virtual interface.

#### add id < external | gre | internal >

adds a virtual interface of the type you specify.

#### external id

configures the external interface.

#### bridge-mode < enable | disable >

enables or disables bridge mode. (If bridge mode is enabled, proxy ARP mode is disabled; if bridge mode is disabled, proxy ARP mode is enabled.)

#### connect

permits a PPPoE/PPTP/L2TP interface to be connected.

#### disconnect

permits a PPPoE/PPTP/L2TP interface to be disconnected.

### **ha-mgmt-ip ip**

sets the virtual IP address that is used to manage the device in a high availability configuration.

### **idle-disconnect < never | 15m | 30m | 1hr | 4hr >**

selects the length of period of inactivity after which the interface will disconnect.

### **igmp [enable | disable] [query-interval seconds] [query-timeout seconds] [max-query-time seconds]**

enables and configures IGMP.

### **local-ip < dhcp | ip netmask mask gw gateway-ip >**

sets the local IP address for connection to the server, either use DHCP or enter the local WAN address of the device, the subnet mask and default gateway.

### **pim-dm < enable | disable >**

enables PIM-DM.

### **release-dhcp-lease**

releases the DHCP lease for the external virtual server's IP address.

### **renew-dhcp-lease**

renews the DHCP lease for the external virtual server's IP address.

### **rip < enable | disable >**

enables or disables RIP on this interface.

### **rip advertise-routes < enable | disable >**

enables or disables the advertisement of RIP routes on this interface.

### **rip auth < disable | simple key | md5 key >**

configures RIP v2 authentication type.

### **rip poison-reverse < enable | disable >**

enables or disables poison reverse.

### **rip receive-mode < disable | v1 | v2 | all >**

configures the RIP receive-mode.

### **rip send-mode < disable | v1 | v2-broadcast | v2-multicast >**

configures the RIP send-mode.

### **rip split-horizon < enable | disable >**

enables split horizon.

### **type < dhcp | < pptp | l2tp > server-ip user username password password | ppoe user username password password | static netmask netmask-IP >**

configures the method by which the external interface can be allocated its IP address.

**zone < add | remove > zone-name**

adds a security zone to (or removes it from) this virtual interface.

### **gre id**

Configures a GRE interface.

**igmp [enable | disable] [ query-interval secs] [query-timeout secs]  
[max-query-time secs]**

Enables and configures IGMP.

**local-ip ip-local**

Configures the IP Address of the tunnel. Choose an unused IP address that is routable through your network

**peer-ip ip**

configures the IP address of the tunnel on the remote device.

**pim-dm < enable | disable >**

enables PIM-DM.

**remote-endpoint-ip remote-ip-address**

configures the IP address of the remote device (the tunnel endpoint) when GRE is not secured by IPSec SA.

**rip < enable | disable >**

enables or disables RIP on this interface.

**rip advertise-routes < enable | disable >**

enables or disables the advertisement of RIP routes on this interface.

**rip auth < disable | simple key | md5 key >**

configures RIP v2 authentication type.

**rip poison-reverse < enable | disable >**

enables poison reverse.

**rip receive-mode < disable | v1 | v2 | all >**

configures the RIP receive-mode.

**rip send-mode < disable | v1 | v2-broadcast | v2-multicast >**

configures the RIP send-mode.

**rip split-horizon < enable | disable >**

enables split horizon.

**sa sa\_name**

configures the IPSec Security Association that the GRE interface will use.

**zone < add | remove > zone-name**

adds a security zone to (or removes it from) this virtual interface. A GRE tunnel requires a security zone in order to function.

**internal id**

Configures an internal interface.

**bridge-mode < enable | disable >**

enables or disables bridge mode. (If bridge mode is enabled, proxy ARP mode is disabled; if bridge mode is disabled, proxy ARP mode is enabled.)

**ha-mgmt-ip ip**

sets the virtual IP address that is used to manage the device in a high availability configuration.

**igmp [enable | disable] [ query-interval secs] [query-timeout secs] [max-query-time secs]**

enables and configures IGMP.

**ip ip netmask netmask**

configures the IP address that you have allocated for this interface and the associated subnet mask.

**nat < disable | external-ip | ip nat-ip >**

enables NAT on this interface.

**pim-dm < enable | disable >**

enables PIM-DM.

**rip < enable | disable >**

enables or disables RIP on this interface.

**rip advertise-routes < enable | disable >**

enables or disables the advertisement of RIP routes on this interface.

**rip auth < disable | simple key | md5 key >**

configures RIP v2 authentication type.

**rip poison-reverse < enable | disable >**

enables poison reverse.

**rip receive-mode < disable | v1 | v2 | all >**

configures the RIP receive-mode.

**rip send-mode < disable | v1 | v2-broadcast | v2-multicast >**

configures the RIP send-mode.

**rip split-horizon < enable | disable >**

enables split horizon.

**zone < add | remove > zone-name**

adds a security zone to (or removes it from) this virtual interface.

**remove id**

Deletes an interface.

---

## Using conf t interface

*create a new  
internal  
interface*

Use **configure terminal interface virtual int** to create a new internal interface. In this example, an internal interface with an ID of 3 is created:

```
hostname# conf t int vi add 3 int
```

The examples that follow assume that the following command has been executed (which puts the CLI into the external interface context):

```
hostname# conf t int vi ext 2
```

*configure  
external  
interface*

Use **type** to configure the external interface. In this example, the interface is set to use L2TP server 1.2.3.4 and DHCP for local communication with a user “jdoe.” The interface will disconnect after 30 minutes of inactivity.

```
hostname(2)# type l2tp 1.2.3.4 user jdoe password bar
hostname(2)# idle-disconnect 30m
hostname(2)# local-ip dhcp
```

*enable RIP*

Use **rip** to enable RIP.

```
hostname(2)# rip enable
```

*configure RIP  
send mode*

Use **RIP send-mode** to configure RIP send mode. In this example, send mode is configured to send updates as RIPv2 multicast.

```
hostname(2)# rip send-mode v2-multicast
```

*add a security  
zone to an  
interface*

Use **zone add** to add a security zone to an interface. In this example, the WAN zone is added to the external interface.

```
hostname(2)# zone add WAN
```

---

## conf t local-user

The **configure terminal local-user** command creates, modifies, removes, or logs out a local user.

**add username privilege-group group-name password password**

adds a local user, assigns a password, and adds the user to a privilege group.

**logout username [ip]**

logs out the specified user. An IP address can be used to further specify the user.

**modify** username [**password** password] [**privilege-group** group-name]

modifies an existing local user.

**remove** username

removes the specified user.

---

### **conf t log audit select**

The **configure terminal log** command enables or disables what is contained in the audit log.

**-all**

sets the log to gather all information.

**boot | no boot**

enables or disables gathering of boot information for the system.

**configuration | no configuration**

enables or disables gathering of configuration information.

**conn-table | no conn-table**

enables or disables gathering of connection table information.

**general | no general**

enables or disables gathering of general information.

**high-availability | no high-availability**

enables or disables gathering of high availability information for the system.

**host | no host**

enables or disables gathering of host information.

**host-communications | no host-communications**

enables or disables gathering of host communication information.

**ip-filter | no ip-filter**

enables or disables gathering of HOST IP filter information.

**login | no login**

enables or disables gathering of login information, such as user accounts and system access.

**logout | no logout**

enables or disables gathering of logout information, such as user accounts and system closing.

**monitor | no monitor**

enables or disables gathering of monitor information, such as packet and network traffic scanning and events.

**oam | no oam**

enables or disables gathering of OAM information.

**policy | no policy**

enables or disables gathering of policy information.

**report | no report**

enables or disables gathering of report information.

**segment | no segment**

enables or disables gathering of segment information, such as port and system settings per segment of a device.

**server | no server**

enables or disables gathering of server information.

**sms | no sms**

enables or disables gathering of SMS information.

**time | no time**

enables or disables gathering of system time information.

**tse | no tse**

enables or disables gathering of information about the Threat Suppression Engine.

**update | no update**

enables or disables gathering of information about system and software updates, such as Digital Vaccine and software updates.

**user | no user**

enables or disables gathering of information about the user, such as account information and access capabilities.

---

**conf t monitor**
**< enable | disable > power-supply**

enables or disables monitoring of the power supply. If any of the power supplies for an IPS device are interrupted, the power supply monitor feature logs a critical message in the system log and sends a notification to the SMS if the device is under SMS management. This feature is available on the following models: 200,400,1200,2400 and 600E, 1200E, 2400E, 5000E.

**threshold**

The configure terminal monitor command enables you to set hardware monitoring thresholds for IPS disk usage, memory, and temperature values. Threshold values represent a percentage and should be between 60-100. Temperature values are displayed as degrees Celsius. When setting thresholds, the major threshold must be set at a value less than the critical threshold value. A major threshold should be set to a value to give you time to react

before a problem occurs. A critical threshold should be set to a value to warn you before a problem causes damage.

**disk** [-major <60-100>] [-critical <60-100>]

sets the threshold for warnings about the disk usage of the device hard disk.

**memory** [-major <60-100>] [-critical <60-100>]

sets the threshold for device memory usage warnings.

**temperature** [-major <40-80>] [-critical <40-80>]

sets the threshold for device temperature warnings.

---

### conf t nms

The **configure terminal nms** command sets the trap IP address, trap port, and SNMP community string for a Network Monitoring System (NMS). The NMS community string is separate from the string used by SMS. **conf t no nms** turns off the NMS options for the system.

**community** NMS-community-string

sets the NMS community string, 1-31 characters.

**no nms**

turns off the NMS options for the system.

**trap-destination** <add | remove > ip [port trap-port]

adds or removes a trap IP address and trap port of the NMS.

---

### conf t notify-contact contact-name agg-period

The **configure terminal notify-contact** command sets the aggregation period of a notification contact. You must enter a name of an existing notification contact and aggregation period (in minutes) for the entry.



**CAUTION:** Short aggregation periods increase system load and can significantly affect system performance. In the event of a flood attack, a short aggregation period can lead to system performance problems.

In this example, the management console aggregation period is set to 2 minutes.

```
hostname# conf t notify-contact "Management Console" 2
```

---

### conf t ntp

The **configure terminal ntp** command configures the NTP settings for the device.

**disable**

turns off NTP timekeeping.

**duration** minutes

interval at which the X family device will check with the time server.

**enable**

turns on NTP timekeeping.

**fast** < **enable** | **disable** >

enables the device to trust the NTP server after the first time query. This sets the local time on the device immediately, but there is a risk that the set time will be incorrect.

**offset** seconds

If the difference between the new time and the current time is equal to or greater than the offset, the new time is accepted by the device. A zero value will force time to change every time the device checks.

**peer** server1[:port1] [server2[:port2] [server3[:port3] [server4[:port4] ] ] ]

sets the IP address of the network peer. The port number default is the IANA NTP port number (123).

**server** server1[:port1] [server2[:port2] [server3[:port3] [server4[:port4] ] ] ]

sets the IP address of the NTP server. The port number default is the IANA NTP port number (123).

---

**Using conf t ntp**

*turn NTP  
timekeeping  
on*

Use **conf t ntp** to enable NTP timekeeping.

```
hostname# conf t ntp enable
```

*turn off NTP  
timekeeping*

Use the **conf t ntp disable** to turn off NTP timekeeping and use the device CMOS clock instead.

```
hostname# conf t ntp disable
```

**conf t port protocol** [add port-number | delete port-number]

The **configure terminal port** command configures additional ports associated with specific applications, services, and protocols to expand scanning of traffic.



**Note:** The following protocols are allowed: auth, dnstcp, dnstcp, finger, ftp, http, imap, ircu, mssql, nntp, pop2, pop3, portmapper, portmapperudp, rlogin, rsh, smb, smtp, snmp, snmpudp, ssh, and telnet.

**conf t profile** profile-name

The **configure terminal profile** command enables you to create, modify, and delete security or traffic management profiles.

**add-pair** [**in** name | **out** name]

adds a security zone pairing to a profile.

**delete**

deletes an existing profile.

**description** description-string

enters a description for the profile.

**remove-pair** [**in** name | **out** name]

removes a security zone pairing from a profile.

**rename** profile-name

renames an existing profile.

**security**

creates a security profile.

---

### Using `conf t profile`

*creating a profile*

In this example, the security profile “LAN WAN” is created, and a security zone pairing is added:

```
hostname# conf t profile "LAN WAN" security
hostname# conf t profile "LAN WAN" add-pair LAN WAN
```

---

### `conf t protection-settings`

The **configure terminal protection-settings** command creates global exceptions and apply-only restriction rules for Application Protection, Infrastructure Protection, and Performance Protection filters.



**Note:** If the profile name contains spaces, it must be enclosed in double quotes; for example:

```
conf t protection-settings app-except add 111.222.33.44
111.222.55.66 -profile "Test Lab"
```

**app-except**

creates a global exception for Application Protection and Infrastructure Protection filters.

**add -profile** profile-name srcIP destIP

adds a global exception for an entered source or destination IP address according to profile.

**remove -profile** profile-name srcIP destIP

removes a global exception for an entered source or destination IP address according to profile.

**app-limit**

creates an apply-only restriction for Application Protection and Infrastructure Protection filters.

**add -profile** profile-name srcIP destIP

adds a global exception for an entered source or destination IP address according to profile.

**remove -profile** profile-name srcIP destIP

removes a global exception for an entered source or destination IP address according to profile.

**perf-limit**

creates an apply-only restriction for Performance Protection filters.

**add -profile** profile-name srcIP destIP

adds a global exception for an entered source or destination IP address according to profile.

**remove -profile** profile-name srcIP destIP

removes a global exception for an entered source or destination IP address according to profile.

---

**conf t ramdisk**

The **configure terminal ramdisk** command configures the synchronization of the RAM disk with the hard disk.

**force-sync** filename

immediately synchronizes the RAM disk with the hard disk, either for all files or for the specified file.

### **sync-interval**

**< alert | audit | block | firewallblock | firewallsession | sys | vpn > seconds**

sets the synchronization interval in seconds for the specified file. A value of 0 means all writes to that file are immediately written to the hard disk. A value of -1 means the specified file is only written to the hard disk under one of the following conditions:

- the user enters a **conf t ramdisk force-sync** command
- the device is rebooted or halted

---

### **conf t remote-syslog**

The **configure terminal remote-syslog** command configures a remote syslog server to record device attack and block messages. Many operating systems and third-party remote syslog packages provide the ability to receive remote syslog messages.



**Note:** Designating a remote syslog server does not automatically send attack and block notifications to that server. You must also select the Remote System Log contact by going to the Filters/Vulnerability filters/Action Sets area in the LSM and either creating or editing an action set. After you apply these changes, active filters that are associated with this action set will send remote messages to the designated server.



**CAUTION:** Only use remote syslog on a secure, trusted network. Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol. It does not offer any additional security protections. You should not use remote syslog unless you can be sure that syslog messages will not be intercepted, altered, or spoofed by a third party.

### **delete ip port**

deletes a remote syslog collector.

### **update ip port**

creates or updates a remote syslog collector. A collector is specified by the required parameters IP address and port, plus a delimiter and facility numbers for alert messages, block messages, and misuse/abuse messages. The facility numbers are all optional.

#### **[-alert-facility 0-31]**

optional facility setting for alert. The range is 0-31.

#### **[-block-facility 0-31]**

optional facility setting for block. The range is 0-31.

#### **[-misuse-facility 0-31]**

optional facility setting for misuse and abuse. The range is 0-31.

#### **[-delimiter < tab | comma | semicolon | bar >]**

setting for the log delimiter. Valid delimiters include tab, comma, semicolon, and bar.

### Using `conf t remote-syslog`

*designate a system to receive remote syslog messages*

Use **configure terminal remote-syslog upd *IP-address*** to designate a remote syslog system. In this example, the remote syslog system is configured on the IP address 1.2.3.4.

```
hostname# conf t remote-syslog upd 1.2.3.4 514
```

*stop sending syslog messages to a remote system*

Use **configure terminal delete** to stop sending syslog messages to a remote system.

```
hostname# conf t remote-syslog delete 1.2.3.4 514
```

### `conf t routing`

The **configure terminal routing** command configures the unit for static, dynamic, and multicast routing.

**multicast igmp < enable | disable >**

globally enables IGMP.

**multicast pim-dm [enable | disable] [query-interval seconds] [prune-timeout seconds]**

globally enables PIM-DM and configures the query interval and the prune timeout.

**rip [enable | disable] [update-timer seconds]**

globally enables RIP and configures the interval between updates of RIP routes to neighbors.

**static-route add ip netmask mask gw gateway [metric number]**

adds a static route.

**static-route remove ip netmask mask**

deletes a static route.

### Using `conf t routing`

*enable RIP*

Use **configure terminal routing RIP** to enable RIP. In this example, RIP is enabled with an update timer of 30 seconds.

```
hostname# conf t routing rip enable update-timer 30
```

*add a static route*

Use **configure terminal static add** to add a static route. In this example, a static route of metric 2 is added to the 192.168.1.0/24 network via 192.168.10.2:

```
hostname# conf t routing static add 192.168.1.0 netmask 255.255.255.0 gw 192.168.10.2 metric 2
```

*enable*  
*PIM-DM*

Use **configure terminal routing** to globally enable PIM-DM.

```
hostname# conf t routing multicast pim-dm enable
```

---

### **conf t server**

The **configure terminal server** command activates and deactivates communications services on the device.



**Note:** When you turn HTTP or HTTPS on or off, you must reboot the device before changes will take effect.



**CAUTION:** The **conf t server** command activates HTTP. HTTP is not a secure service. If you enable HTTP, you endanger the security of the device. Use HTTPS instead of HTTP for normal operations.

The SMS requires HTTPS communications. If you turn off the HTTPS server, the SMS will not be able to manage the device.

#### **browser-check | no browser-check**

enables or disables browser checking. For browser compatibility information, refer to the *LSM User's Guide*.

#### **http | no http**

enables or disables the HTTP server.

#### **https | no https**

enables or disables the HTTPS server.

#### **ssh | no ssh**

enables or disables the SSH server.

---

### **conf t service-access**

The **configure terminal service-access** command enables and disables a special remote access user login that can be used by a technical support representative to retrieve diagnostic information. This login only functions when you enable it, and it will be deleted once the technical support representative logs out. If you need technical support again in the future, you must reissue the command. **conf t no service-access** disables the remote access login.



**Note:** When you issue the configure terminal service-access command, the device will return the serial number and a "salt" value. You must retain these numbers for the technical support representative.

*enable  
technical  
support  
diagnostic  
access*

Use **configure terminal service-access** to enable technical support diagnostic access to the device.

```
hostname# conf t service-access
```

*disable  
technical  
support  
diagnostic  
access*

Use **configure terminal no service-access** to disable technical support diagnostic access to the device.

```
hostname# conf t no service-access
```

---

### conf t session

The **configure terminal session** command configures the display of the CLI session on your management terminal. This command is enabled when the SMS manages the device. The command abbreviation is **conf t sess**.

These commands are not persistent and session changes will be lost when you log out. Only super-users can create a persistent **timeout** option.

#### **columns** *columns*

sets the column width of the terminal session.

#### **more**

enables page-by-page output to the terminal screen. **no more** disables page-by-page output to the terminal screen. The output appears as one continuous stream of text.

#### **rows** *rows*

controls the height of the session display by number of rows.

#### **timeout** *minutes* **[-persist]**

sets the inactivity timeout for the CLI session. The **-persist** option is super-user only, and it applies the specified timeout value to all future sessions for all users as well as the current session.

#### **wraparound**

controls text-wrapping for text longer than the set width of the session. The text is wrapped. **no wraparound** turns off the text-wrapping option. The text is truncated.

---

### Using conf t session

*configure  
session  
settings*

Use **configure terminal session** to configure session settings. In the following example, the display is set to a size of 80 columns by 40 rows, page-by-page display, and wrapped text. The session will time out after 25 minutes.

```
hostname# conf t session columns 80
hostname# conf t session more
hostname# conf t session wrap
hostname# conf t session rows 40
```

```
hostname# conf t session timeout 25
hostname# show session
Current Session Settings
Terminal Type           = Console
Screen width            = 80
Screen height           = 40
Hard wrap                = Enabled
More                    = Enabled
Session Timeout         = 25
```

---

### conf t sms

The **configure terminal sms** command enables or disables SMS management of the device and configures communications with the SMS. **conf t no sms** turns off SMS management and restores local control to the device.

#### ip ip [port <0-65535>]

the IP address and port of the SMS that you want to monitor the device.

#### must-be-ip ip

restricts SMS management to the specified IP address or CIDR range. Only the SMS with this IP can manage the device. **no must-be-ip** turns off SMS restriction, allowing any SMS to manage the device.

#### remote-deploy primary-ip-address secondary-ip-address [-fallback]

enables configuration of the device by a primary and optional secondary SMS device, specified by IP address. When the command is executed, the device will initiate a call to the SMS to begin the acquisition of the configuration files. **conf t sms no remote-deploy** disables the remote deployment.

When the SMS is on a different site than the device, a potential misconfiguration in the SMS may result in the loss of remote management access to the device. To protect against this, you can use **-fallback** to enable a firewall rule to allow SSH and HTTPS access into the device from the WAN security zone and the Internet. This rule will only be enabled after the SMS has timed out trying to acquire the device. While the rule is enabled, management access to the device is available from any IP address on the Internet providing the correct username and password.

For more information about remote deployment, refer to the *SMS User's Guide*.

#### v2 | no v2

enables or disables SNMP v2 communications.

---

### Using conf t sms

#### *enable sms management*

Use **conf t sms** to enable SMS management of the device. In this example, the command enables the SMS device at the IP address 111.222.34.200 to manage the device:

```
hostname# conf t sms ip 111.222.34.200
```

*enable remote deployment*

Use **conf t sms remote-deploy** to enable configuration of the device by a remote SMS. In the first example, the device will be configured by the SMS with the IP address 111.222.34.200:

```
hostname# conf t sms remote-deploy 111.222.34.200
```

In the next example, configuration by primary and secondary SMS devices is enabled. The primary SMS IP address is 111.222.34.200, and the secondary SMS IP address is 111.222.34.201:

```
hostname# conf t sms remote-deploy 111.222.34.200 111.222.34.201
```

*disable sms management*

Use **conf t no sms** command to turn off SMS management of the device.

```
hostname# conf t no sms
```

**conf t tse**

The **configure terminal tse** command configures settings for the Threat Suppression Engine (TSE).

**adaptive-filter mode [automatic | manual]**

sets the adaptive filter mode to automatic or manual for the TSE.

**afc-severity [critical | error | warning | info]**

sets the severity of messages logged by the Adaptive Filter Configuration (AFC).

**connection-table timeout <30-1800>**

defines the global connection table timeout in seconds. The range is 30 to 1800 seconds.

**logging-mode conditional [-threshold nn.n] [-period seconds]**

enables improved performance by turning off alert/block logging when the device experiences a specified amount of congestion. This feature is enabled by default.

The **-threshold** setting configures the percentage of packet loss that turns off logging. The **-period** setting configures the amount of time logging remains off.

**logging-mode unconditional**

enables logging even when traffic is dropped under a high load. This command disables the threshold option for disabling alert and block logging when a specified amount of congestion passes through the device.

**quarantine duration minutes**

specifies the length of time for which a host will remain on the quarantine list when it is identified by the device, SMS, or an administrator as having a security issue.

**conf t user**

The **configure terminal user** command configures user accounts. All users can change their own passwords, but the majority of the command functionality is limited to super-users. This command is enabled even when the SMS manages the device.

### **add** *username*

adds a user account to the system. You can add the password and role for the account with the following flags.

#### **-password** *password*

enters a password for the account. If you do not include the password on the command line, you will be prompted for the password after entering the **configure terminal user add** command.



**Note:** Do not use quotation marks in passwords. Quotation marks are treated differently depending on how they are entered and where they are placed within a password and may lead to confusion when attempting to log on to the device.

#### **-role < operator | admin | super-user >**

assigns a user access role to the new user account.

### **enable** *name*

enables users who have been disabled by lockout or expiration. **no enable** *name* disables a user account.

### **modify** *name*

modifies an existing user account.

#### **[-password** *password*]

enters a password for the account. If you do not include the password on the command line, you will be prompted for the password after entering the **configure terminal user modify** command.

#### **-role < operator | admin | super-user >**

assigns a user access role to the user account.

### **options**

configures the security options for all user accounts on the device. If you use the **conf t user options** command without any parameters, it displays the current settings.

#### **attempt-action**

controls how an device handles an account after the max-attempts setting is exceeded. An attempt is recorded when an invalid password entry is submitted.

#### **disable**

disables the account when **max-attempts** is exceeded. A super-user must re-enable the account with the **conf t user enable** command.

#### **lockout**

locks out an account for the period of time specified in **lockout-period** when **max-attempts** is exceeded.

#### **expire-action**

configures the actions that the device takes on an account when a password expires.

**disable**

disables the account when **expire-period** is reached. A super-user must re-enable the account.

**expire**

expires the account when **expire-period** is reached. The user must enter a new password when logging on.

**notify**

nothing is done to the account. The user is notified that the account is expired and the user should change the password

**expire-period** days

sets the period of time in days that account passwords are valid. The **expire-action** setting controls what happens next to the account. Valid periods, in days, include 0, 10, 20, 30, 45, 90, 332, and 365.

**lockout-period** minutes

sets a lockout period on a user account. Valid periods, in minutes, include 0, 1, 5, 10, 30, 60, and 360.

**max-attempts** <1-10>

sets the number of maximum login attempts on a single account. The **attempt-action** setting configures the action that occurs when **max-attempts** is exceeded. The valid number of attempts is an integer from 1 to 10.

**security-level** <0-2>

sets the level of security checking that is performed when you add a new user or change a password. Enter a level value of 0, 1, or 2.

The restrictions for the security levels includes the following:

**Table 3-1: Security Levels**

| Level   | Description                                                                                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Level 0 | User names cannot have spaces in them.<br>Passwords are unrestricted.                                                                                                        |
| Level 1 | User names must be at least 6 characters long without spaces.<br>Passwords must be at least 8.                                                                               |
| Level 2 | Includes Level 1 restrictions and requires the following: 2 alphabetic characters, 1 numeric character, 1 non-alphanumeric character (special characters such as ! ? and *). |



**CAUTION:** Using any security level less than 2 is counter to accepted business practice. If you use a security level less than 2, the security of the device may be easily compromised by a password guessing program.

**user remove username**  
removes a user account.

---

### Using `cft user`

*add a new user*

Use **configure terminal user add** to add a new user. In this example, the user **kwalker** is added with the password **tap2-tap2**:

```
hostname# cft user add kwalker -role super -password tap2-tap2
```

*enable a user who has been locked out*

Use **cft user enable** to enable a user who has been locked. In this example, the account **kwalker** is enabled:

```
hostname# cft user enable kwalker
```

*disable a user*

Use **cft user no enable** to disable a user. In this example, the account **kwalker** is disabled:

```
hostname# cft user no enable kwalker
```

*change security checking level*

Use **cft user options security-level** to change the security checking options. In this example, the security level is changed to Level 2:

```
hostname# cft user options security-level 2
```

*disable or lockout account after action is attempted many times*

Use **cft user option attempt-action** to set the option to disable or lockout an account after repeated and invalid attempts.

```
hostname# cft user option attempt-action disable
```

```
hostname# cft user option attempt-action lockout
```

*disable an account when it expires*

Use **cft user option expire-action disable** to set the option to disable an account when the password expires.

```
hostname# cft user option expire-action disable
```

*expire a user when account expires*

Use **cft user option expire-action expire** to set the option to expire an account when the password expires.

```
hostname# cft user option expire-action expire
```

*notify a user when account expires*

Use **cft user option expire-action notify** to set the option to notify a user when the password expires.

```
hostname# cft user option expire-action notify
```

*expire an account after 10 days*

Use **cft user option expire-period** to cause accounts to expire after a set number of days. In this example, this option will expire accounts after 10 days.

```
hostname# cft user option expire-period 10
```

*locks out an  
account for  
three minutes*

Use **cft user option lockout-period** to set the number of minutes that a user is locked out after the maximum number of failed login attempts. In this example, the lockout period is 3 minutes:

```
hostname# cft user option lockout-period 3
```

*locks out an  
account after  
five attempts*

Use **cft user option max-attempts** to set the maximum number of failed login attempts on user accounts. In this example, the maximum number of attempts is 5:

```
hostname# cft user option max-attempts 5
```

*change the  
password  
expiration  
period*

Use **cft user options expire-period** to change the password expiration period. In this example, the expiration period is 30 days:

```
hostname# cft user options expire-period 30
```

*remove a user  
login*

Use **cft user remove** to remove a user account. In this example, the account **kwalker** is removed:

```
hostname# cft user remove kwalker
```

---

### conf t vpn debug

The **configure terminal vpn debug** command control VPN debugging.

#### logging < disable | enable >

disables or enables logging of all VPN-related events to the system log.

---

### conf t vpn ike

The **configure terminal vpn ike** command adds and configures Internet Key Exchange (IKE) proposals.

#### add proposal-name

adds an IKE proposal.

#### local-id [domain domain-name email email-address]

configures the local ID with a domain name and email address.

#### proposal proposal-name

takes you into the context of that IKE proposal.

#### aggressive-mode < enable | disable >

enables aggressive mode for authentication.

#### auth-type < psk | x509 >

selects the authentication type: pre-shared key or X.509 certificates.

#### auto-connect < enable | disable >

enables phase 1 auto-connect. Use auto-connect if you want to initiate the VPN upon startup with IKE phase 1 proposals automatically established.

### **auto-connect-phase2 < enable | disable >**

enables phase 2 auto-connect. Use auto-connect if you want to initiate the VPN on startup with IKE phase 2 proposals automatically established.



**Note:** To enable phase 2 auto-connect, phase 1 autoconnect (**auto-connect enable**) must also be enabled.

### **ca-cert < any | certificate-name >**

specifies the name of the CA certificate, if you are using certificates for authentication.

### **dpd < enable | disable >**

enables dead peer detection.

### **local-id-type < ip | email | domain | dn >**

configures the identifier that the device will use for validation purposes. Use this if you are using pre-shared key with aggressive mode. This identifier must match the remote Peer ID Type.



**Note:** The local IDs for the email address and domain name types are configured in the IKE Proposal. The local ID for the IP address type is the WAN IP address.

### **local-x509-cert certificate-name**

specifies the name of the local certificate if you are using certificates for authentication.

### **nat-t < enable | disable >**

enables NAT-Transversal. Use NAT-Transversal if there is a NAT device between the two VPN devices.

### **peer-id-type < ip | email | domain | dn >**

selects the identifier for the device to use for validation purposes, either IP address, email address or domain name. This must match the local ID type.

### **pfs < enable | disable >**

enables or disables Perfect Forward Secrecy.

### **phase1-dh-group < 1 | 2 | 5 >**

selects the Diffie-Hellman group number for IKE phase 1.

### **phase1-encryption < des-cbc | 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 >**

configures encryption for IKE phase 1. Some options are only valid on the High Encryption agent, which can be downloaded from the TMC.

### **phase1-integrity < md5 | sha1 >**

configures integrity for IKE phase 1.

**phase1-lifetime < 600–999999 >**

selects the length of time in seconds you want the Security Association to last before new authentication and encryption keys must be exchanged (between 600 and 999999 seconds, default 28800).

**phase2-dh-group < 1 | 2 | 5 >**

selects the Diffie-Hellman group number for IKE phase 2.

**phase2-encryption < null | des-cbc | 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 >**

configures encryption for IKE phase 2. Some options are only valid on the High Encryption agent, which can be downloaded from the TMC.

**phase2-integrity < none | esp-sha1-hmac | esp-md5-hmac | ah-md5 | ah-sha1 >**

configures integrity for IKE phase 2.

**phase2-lifetime < 300–999999 >**

selects the length of time in seconds you want the Security Association to last before new authentication and encryption keys must be exchanged (between 300 and 999999 seconds, default 3600).

**phase2-strict-id-check < enable | disable >**

enables or disables strict ID checking.

**phase2-zero-id < enable | disable >**

enables the IP subnet tunnels without specified local and remote IDs. When this option is enabled, administrators must control traffic through the routing configuration and firewall rules.

**tight-phase2-control < enable | disable >**

when enabled, improves interoperability with VPN devices that automatically delete all the phase 2 Security Associations when the phase 1 Security Association terminates.

**remove name**

deletes an IKE proposal.

---

**Using conf t vpn ike**

*configure local ID to be a domain name or email address*

Use **configure terminal vpn ike local-id** to configure the local ID as a domain name or email address. In this example, the domain name is set as **xyz.com** and then the email address is set as **jdoe@xyz.com**:

```
hostname# conf t vpn ike local-id domain xyz.com
hostname# conf t vpn ike local-id email jdoe@xyz.com
```

*name an IKE proposal and enter its context*

Use **configure terminal vpn ike proposal** to create an IKE proposal, which also opens the context for that proposal. In this example, an IKE proposal named **london** is created, and the next command line is in the context of that proposal:

```
hostname# conf t vpn ike add london
hostname# conf t vpn ike proposal london
hostname(london)#
```

*configure phase 1 encryption*

Use **phase1-encryption** within the context of the IKE proposal to configure phase 1 encryption. In this example, phase 1 encryption to 3DES-CBC is set in the context of the proposal named **london**:

```
hostname# conf t vpn ike proposal london
hostname(london)# phase1-encryption 3des-cbc
```

---

### **conf t vpn ipsec**

The **configure terminal vpn ipsec** command configures an IPSec VPN tunnel.



**Note:** The name “Default” represents the default SA (Security Association).

In the command-line interface, you cannot renegotiate or delete a Security Association terminating on the device if that device did not initiate that Security Association.

#### **add name**

configures the name for a new Security Association.

#### **disable**

disables IPSec.

#### **enable**

enables IPSec.

#### **remove name**

deletes the configuration of a Security Association.

#### **sa name**

takes you into the context of the named Security Association.

#### **delete**

brings down any tunnels using this Security Association.

#### **disable**

disables this Security Association.

#### **enable**

enables this Security Association.

**key**

selects and configures the keying mode. Some options are only valid on the High Encryption agent, which can be downloaded from the TMC.

**manual incoming-spi** spi **outgoing-spi** spi **encryption**  
**< des-cbc | 3des-cbc | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 >**  
**authentication <esp-sha1-hmac | esp-md5-hmac | ah-md5 | ah-sha1>**  
**encryption-key** key **auth-key** key  
 configures manual mode.

**ike proposal** proposal-name [**shared-secret** secret] [**peer-id** id]  
 configures IKE proposal. If included, the shared secret must be at least 8 characters long.

**negotiate**

starts negotiation of the tunnel.

**peer ip**

configures the IP address of the terminating VPN unit or network device (the remote target of the VPN link).

**transport < enable | disable >**

enables or disables transport mode. Use this if you are using L2TP or if you are configuring a Security Association to use with a GRE interface.

**tunnel**

controls tunneling.

**disable**

disables tunneling.

**enable**

enables tunneling.

**local < default-route | dhcp | group** group-name |  
**subnet ip netmask** netmask | **range** ip1 ip2 >

select the source IP addresses that are allowed to use this IPSec tunnel by specifying an IP address group, subnet, or range. You should use an IP address group that contains all the source IP addresses of devices that can use the IPSec tunnel.

Choose **default-route** if the remote IPSec peer uses this IPSec tunnel as its default route. Choose **dhcp** if the local network devices receive IP addresses by DHCP over this IPSec tunnel. DHCP relay must first be configured to use this tunnel before selecting this option.

**nat < disable | ip >**

enables or disables NAT tunneling.

**remote** < **default-route** | **dhcp** | **group** group-name |  
**subnet** ip **netmask** netmask | **range** ip1 ip2 >

select the destination IP addresses that can be reached over this IPSec tunnel by specifying an IP address group, subnet, or range.

Choose **default-route** if this device uses this IPSec tunnel as its default route for all network traffic that does not have a more specific route. Choose **dhcp** if the remote device receives IP addresses by DHCP over this IPSec tunnel.

**zone** zone

specify the security zone on which you want the VPN terminated.

---

### Using `conf t vpn ipsec`

*create and  
enter the  
context of an  
SA*

Use **configure terminal vpn ipsec sa** to create and enter the context of a Security Association. In this example, an SA called **tunnelone** is created. The next command line is within the context of the SA.

```
hostname# conf t vpn ipsec add tunnelone
hostname# conf t vpn ipsec sa tunnelone
hostname(tunnelone)#
```

*configure the  
IP address of  
the IPSec  
gateway*

Use **peer** in the context of an SA to configure the IP address of the IPSec gateway. In this example, the IPSec gateway 192.168.1.5 is configured within the context of the SA **tunnelone**:

```
hostname(tunnelone)# peer 192.168.1.5
```

*configure the  
termination  
zone*

Use **zone** within the context of an SA to configure the security zone where a VPN tunnel will terminate. In this example, the termination zone is set to LAN within the context of the SA **tunnelone**:

```
hostname(tunnelone)# zone LAN
```

*configure the  
keying mode*

Use **key** within the context of an SA to configure the keying mode. In this example, set in the context of the SA **tunnelone**, the keying mode is set to IKE with the proposal **ike-proposal1**, the peer ID is **xyz.abc.com** and the shared secret is **bananas!**:

```
hostname(tunnelone)# key ike proposal ike-proposal1 peer-id xyz.abc.com
shared-secret bananas!
```

*configure the  
destination  
network*

Use **tunnel** within the context of an SA to set the destination network of the tunnel. In the example, the destination network is configured on the subnet 192.168.2.0 and netmask 255.255.255.0:

```
hostname(tunnelone)# tunnel subnet 192.168.2.0 netmask 255.255.255.0
```

---

### `conf t vpn l2tp`

The **configure terminal vpn l2tp** command configures an L2TP VPN connection.

**addresses < radius | group name | none >**

configures how L2TP addresses are assigned. Either specify **none**, specify a RADIUS server, or specify an IP address group from which to have addresses assigned.

**disable**

disables the L2TP server.

**dns < relay | server-ip-1 [server-ip-2] >**

configures DNS servers. Use **relay** if you want the device to act as a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers. You can also specify up to two DNS server IP addresses.

**enable**

enables the L2TP server.

**encryption < enable | disable >**

enables Microsoft Point-to-Point Encryption.

**logout username [ip]**

forces a logout of the named user or the named IP address.

**wins server-ip-1 [server-ip-2]**

specifies the IP addresses of the primary and secondary WINS servers (if you are using Microsoft Networking).

**zone zone-name**

selects the remote security zone on which to terminate the VPN.

---

**Using conf t vpn l2tp**

*configure  
address group  
for L2TP  
clients*

Use **configure terminal vpn l2tp addresses** to configure the address group from which L2TP clients will be assigned their IP addresses. In this example, addresses are assigned from an address group called **l2tp**:

```
hostname# conf t vpn l2tp addresses group l2tp
```

*configure a  
termination  
zone for L2TP  
clients*

Use **configure terminal vpn l2tp zone** to configure the security zone where L2TP clients will terminate. In this example, clients will terminate in the LAN zone:

```
hostname# conf t vpn l2tp zone LAN
```

---

**conf t vpn pptp**

The **configure terminal vpn pptp** command configures a PPTP VPN connection.

**addresses < radius | group name | none >**

configures how PPTP addresses are assigned. Either specify **none**, specify a RADIUS server, or specify an IP address group from which to have addresses assigned.

### **disable**

disables the PPTP server.

### **dns < relay | server-ip-1 [server-ip-2] >**

configures DNS servers. Use **relay** if you want the device to act as a proxy-DNS server (DNS relay), passing DNS queries to its configured DNS servers, or specify up to two DNS server IP addresses.

### **enable**

enables the PPTP server.

### **encryption < disable | enable >**

enables Microsoft Point-to-Point Encryption.

### **logout username [ip]**

logs out the named user or the named IP address.

### **wins server-ip-1 [server-ip-2]**

specifies the IP addresses of the primary and secondary WINS servers (if you are using Microsoft Networking).

### **zone zone-name**

specifies the remote security zone on which to terminate the VPN.

---

## Using `conf t vpn pptp`

*configure  
address to be  
assigned by  
RADIUS*

Use **configure terminal vpn pptp addresses** to configure the VPN connection to assign addresses to clients from a RADIUS server.

```
hostname# conf t vpn pptp addresses radius
```

*configure DNS  
servers for  
PPTP clients*

Use **configure terminal vpn pptp dns** to configure DNS servers for PPTP clients. In this example, DNS servers at 192.168.1.2 and 192.168.1.3 are configured:

```
hostname# conf t vpn pptp dns 192.168.1.2 192.168.1.3
```

---

## **conf t web-filtering**

The **configure terminal web-filtering** command is the parent command for all web content-filtering related options. The command must be used with a subcommand.

### **default-rule < permit | block >**

configures the device response to a request for a web site that is not a member of a currently filtered category or covered by a Manual Filtering rule. The default rule can be set to **permit**, which serves the request and allows access, or to **block**, which blocks the request and blocks access. This rule is also applied when the Content Filter Service is not licensed, or the CPA (Content Portal Authority) server cannot be contacted by the device.

**filter-action < block | log | block-and-log >**

specifies the actions that occur when a web request is filtered. The device can block web requests, log them in the device's system log, or both block and log them. Filtering actions apply to both the filtering service and manual filtering mode.

**filter-service cache**

configures the web filter cache.

**expiry** hours

configures the number of hours that the web filter cache will retain web pages.

**size** bytes

configures the size of the web filter cache in bytes.

**filter-service < enable | disable >**

enables the subscription-based Content Filter Service.

**filter-service < permit | block > category-name**

permits or blocks a Content Filtering Service category.

**filter-service server < america | europe1 | europe2 | asia | address address >**

specifies the content filtering server that will provide the Content Filter Service.

**manual-filter < add | remove > < permit | block >****< string | regexp > string-or-expression**

configures the manual filter. You can add or remove, a combination of URLs, domain names, IP addresses, keywords, and regular expressions to determine which web requests are permitted or blocked.

**manual-filter < enable | disable >**

enables or disables manual filtering.

---

**Using conf t web-filtering**
*add a manual filtering rule*

Use **configure terminal content-filtering manual-filter add permit** to add a manual web filtering rule. In this example, URLs containing the string **google** are permitted:

```
hostname# conf t web-filtering manual-filter add permit string google
```

*delete a manual filtering rule*

Use **configure terminal content-filtering manual-filter remove** to delete a manual filtering rule. In this example, the rule created in the example above is removed:

```
hostname# conf t web-filtering manual-filter remove permit string google
```

*permit a category*

Use **configure terminal content-filtering filter-service** to permit or block categories in the Content Filtering Service. In this example, all web sites and domains in the **gambling** category are permitted:

```
hostname# conf t web-filtering filter-service permit gambling
```

**conf t zone**

Use the **configure terminal zone** command to create and configure security zones on the device.

**add** zone-name

adds the named security zone.

**remove** zone-name

deletes a security zone.

**update** zone-name

updates the named security zone.

**addresses** < disable | group group-name | subnet ip netmask mask |**range** ip1 ip2 >

specifies the devices that are permitted inside a security zone by group, subnet, or IP address range.

**bandwidth** [ outbound <1–100000> ] [ inbound <1–100000> ]

configures the bandwidth for the security zone in kbps.

**mtu** mtu

specifies the MTU number.

**ports** < [slot/port [slot/port] ...] [vlan-tagged slot/port [slot/port] ...] ] | none >

designates the ports on which the security zone exists, and which port, if any, is tagged with VLAN.

**vlan-id** vlan-ID-number

specifies the VLAN ID number, if used.

**vpn-tunnel-access** < enable | disable >

enables or disables VPN tunnel access to the security zone.

**Using conf t zone***update a  
Security Zone*

Use **configure terminal zone update** to modify a security zone. In this example, the security zone LAN is updated with port 1 from slot 3 and 2 from slot 3 un-tagged, and port 4 from slot 3 vlan-tagged:

```
hostname# conf t zone update LAN ports 3/1 3/2 vlan-tagged 3/4
```

*configure  
network  
protection*

Use **configure terminal zone update addresses** to restrict the devices permitted inside a security zone to a particular subnet. In this example, only devices on the subnet 192.168.10.0/24 are permitted inside the security zone:

```
hostname# conf t zone update LAN addresses subnet 192.168.10.0 netmask  
255.255.255.0
```

**debug**

access: super user

Most debug commands should only be used when you are instructed to do so by technical support, but some commands can be useful in managing the device.

**factory-reset**

The **debug factory-reset** command returns the device to its factory defaults.



**CAUTION:** Use this command only when instructed to do so by technical support.

**log syslog**

The **debug log syslog** command is used to review syslog server settings.

**audit ip**

reviews the settings of the audit log on the syslog server. Specify the IP address of the server that you want to review.

**systemlog ip**

reviews the settings of the system log on the syslog server. Specify the IP address of the server.

**exit**

access: global; all

The **exit** command backs you out of one level of submenu or, if you use **exit all**, backs you out of all submenus. For more information about sub-menus and local commands, see [Chapter 4, “Navigation”](#).

**Using exit**

*back out of  
one menu  
level*

Use **exit** to back out of one submenu. In this example, the user moves from the **cfg-server** level to the **config** level:

```
hostname(cfg-svr)# exit
hostname(config)#
```

*back out of all  
submenus*

Use **exit all** back out of all submenus.

```
hostname(cfg-svr)# exit all
```

```
hostname#
```

### halt

access: local; super-user, admin

The **halt** command shuts down the device.

**seconds**

instructs the device to wait from 0-3600 seconds before initiating the halt sequence.

**now**

instructs the device to halt immediately.

*shut down X  
Family device*

Use **halt** to shut down the device.

```
hostname# halt
Are you sure you want to halt the system? <Y,[N]>:y
hostname#
Achieved RunLevel 0

Safe to power-off
```

### help

access: global; all

The help command shows brief descriptions of keyboard editing commands and global commands.

**edit**

shows the keyboard editing commands.

**commands**

lists the global commands.

### high-availability

access: admin

The **high-availability** command sets the high availability status of the device.

---

**force active**

forces the device into Active state.

**force standby**

forces the device into Standby state.

**history**

access: global; all

The **history** command displays the last 30 commands typed from the command line. The command abbreviation is **hist**.

The history command can be used in combination with the **!** command to execute a command in the history buffer.

**Using history**

*view history  
(command)  
buffer*

Use **history** to view the commands in the history buffer.

```
hostname# history
1 show chassis
2 show session
3 conf term
```

*execute  
command  
<number>  
from history  
buffer*

Use **history** followed by **!** and a number execute a particular command from the history buffer. In this example, the second command in the buffer is executed:

```
hostname# hist
1 ls
2 show clock
3 conf t sess wrap
4 hist
hostname# !2
hostname# show clock
Local Time: 2002-05-01 12:14:12
Timezone: CDT
DST: disabled
```

**logout**

access: global; all

The **logout** command logs you off of the device.

**Using logout**

*log off the  
device*

Use **logout** command to log off of the device.

```
hostname# logout
```

### ping

access: global; all

The **ping** command tests whether you can reach a particular IP address and how long it takes to receive a reply.

**ip**

selects the destination IP address.

**count**

the number of packets to send.

**-d**

specifies reverse DNS lookup on responding IP address.

**-i**

specifies the interval between packets.

**-q**

suppresses statistics.

**-R**

records the route.

**-t**

specifies theTTL to use.

**-v**

sets verbose format.

*test whether  
you can reach  
a particular  
IP address*

Use **ping** test whether you can reach a particular IP address. In this example, the IP address 111.222.34.200 is tested:

```
hostname# ping 111.222.34.200
PING 111.222.34.200: 56 data bytes
64 bytes from 111.222.34.200: icmp_seq=0. time=0. ms
64 bytes from 111.222.34.200: icmp_seq=1. time=0. ms
64 bytes from 111.222.34.200: icmp_seq=0. time=0. ms
64 bytes from 111.222.34.200: icmp_seq=1. time=0. ms
64 bytes from 111.222.34.200: icmp_seq=0. time=0. ms
----111.222.34.200 PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
```

**quarantine**

access: global; all

The **quarantine** command displays a list of quarantined hosts, and is used to add hosts to or remove hosts from from the list.

**add ip "action-set"**

adds a device to the list of quarantined devices.

**empty**

removes all devices from quarantine.

**list [filter ip]**

lists all devices that are quarantined, or those quarantined within a particular range of IP addresses that you specify using **filter**.

**remove ip**

removes the device at the specified IP address from quarantine.

**quit**

access: global; all

The **quit** command logs you out of the CLI. After the command is executed, a Login prompt is displayed.

**Using quit**

*log out of the  
CLI*

Use **quit** to log out of the CLI.

```
hostname# quit
Login:
```

**reboot**

access: local; super, admin

The **reboot** command reboots the system software. If you use **reboot** without any parameters, the device will initiate the reboot in 5 seconds.

**seconds**

instructs the device to begin the reboot process in from 0 to 3600 seconds.

---

### now

instructs the device to reboot immediately.

---

### Using reboot

*reboot the device*

Use the reboot to reboot the system. You will be asked to confirm the command. Enter **Y** to proceed with the reboot, enter **N** to cancel the reboot.

```
hostname# reboot
Are you sure you want to reboot the system? <Y,[N]>: Y
Broadcast message from kscanlon

Rebooting local processor in 5 seconds...
```

---

### setup

access: local; super, admin (time for super only)

The **setup** command invokes setup wizards for default email, Ethernet port, NMS, Web/CLI/SNMP servers, restricted SMS, and time settings. If you use the setup command without any parameters, it will execute all of the wizards. For detailed information on the setup command and wizards, see [Chapter 1, “X Family Startup Configuration”](#).

---

### show

access: local; all (except log audit), log audit - super

The show command displays current system configuration, status, and statistics.



**Note:** There are two important forms of the **show** command, which offer different information:

- **show** retrieves information from the component itself and provides the current status of a device hardware or software component.
- **show configuration** retrieves information from the configuration files and provides the current entries in the device configuration files.

### show action-sets

The **show action-sets** command lists the action sets.

```
hostname# show action-sets
```

| Action Set Name     | Action             | TCP Reset | Pkt Trace | Channel            |
|---------------------|--------------------|-----------|-----------|--------------------|
| -----               | -----              | -----     | -----     | -----              |
| Block+Notify+Trace  | Block              |           | Enabled   | Management Console |
| Block               | Block              |           |           |                    |
| Recommended         | Category Dependent |           |           |                    |
| Block + Notify      | Block              |           |           | Management Console |
| Permit+Notify+Trace | Permit             |           | Enabled   | Management Console |
| Permit + Notify     | Permit             |           |           | Management Console |

### show arp

The **show arp** command shows the link level ARP table.

```
hostname# show arp
```

| Link Level ARP table |                         |           |            |
|----------------------|-------------------------|-----------|------------|
| Destination IP       | Destination Mac Address | Interface | Entry Type |
| -----                | -----                   | -----     | -----      |
| 192.168.1.254        | 00:50:c2:12:1e:29       | 1         | Permanent  |
| 10.0.3.100           | 00:10:f3:01:eb:58       | 2         | Dynamic    |
| 10.0.3.200           | 00:50:c2:12:1e:28       | 2         | Permanent  |

### show autodv

The **show autodv** shows the settings for the automatic updating of Digital Vaccine files.

### show chassis [-details]

The **show chassis** command shows configuration and status information, including slot, module type, configuration, state, and qualifier status. Use **show chassis** alone to view all slots and modules. Use **show chassis -slot <1-8>** to view a single module. Add the **-detail** flag to get additional qualifier and port quantity information.

#### -details

the **-details** flag can be used either with the **show chassis** or **show chassis -slot <1-8>** command

### Using show chassis

#### show all slots

Use **show chassis** with no parameters to show the status of the modules in all chassis slots.

```
hostname# show chassis
```

Serial: : X-X5-STLAB-0005

| Slot Type | Config | State | Qual-1 | Qual-2 |
|-----------|--------|-------|--------|--------|
| -----     | -----  | ----- | -----  | -----  |

```
SLT1 Management Processor   Simplex Active           No Info  No Info
SLT3 Port Health           Simplex Active           No Info  No Info
SLT5 Threat Suppression Eng Simplex Active           No Info  No Info
```

*show all slots  
with more  
detail*

Use **show chassis -details** to show the status of a single module with more detail.

```
hostname# hostname# show chassis -details
Serial:      : X-X5-STLAB-0005
```

| Slot | Type            | Config  | State  | Qual-1  | Qual-2  | Ports |
|------|-----------------|---------|--------|---------|---------|-------|
| SLT1 | Management Proc | Simplex | Active | No Info | No Info | 1     |
| SLT3 | Port Health     | Simplex | Active | No Info | No Info | 4     |
| SLT5 | Threat Suppress | Simplex | Active | No Info | No Info | 0     |

### show clock

The **show clock** command shows the local time, the timezone setting, and the daylight saving time setting.

#### -details

adds information about timezone offsets, UTC (Universal Time), and whether the clock is under NTP or local control.

### Using show clock

*show local  
time,  
timezone  
setting, and  
daylight  
saving time  
setting*

Use **show clock** to show the local time, the timezone, and the daylight saving time setting.

```
hostname# show clock
Local Time: 2007-04-30 12:23:01
Timezone: CST
DST: disabled
```

*show local,  
timezone, and  
universal time  
information*

Use **show clock -details** to show local, timezone, and universal time information.

```
show clock -details
Local Time: 2007-04-30 15:15:47
Timezone: CST
DST: disabled
TIMEZONE: CST::360:040702:102702
UTC: 2007-04-30 20:15:47
Clock Master: NTP
```

### show configuration

The **show configuration** command shows persistent configuration settings on the device. The command abbreviation is **show conf**.

Show configuration commands can be used to feed configuration information back to the console. Without parameters, the command shows the system's configuration.

### **action-set**

lists all action sets that have been defined for this device. Can be changed with [conf t action-set action-set-name threshold threshold-period](#).

### **address-group**

shows the configuration of the address group or groups. Can be changed with [conf t address-groups](#).

### **authentication [radius | privilege-group]**

shows authentication configuration.

### **autoDV**

shows configuration settings for the automatic update service for Digital Vaccine packages. Can be changed with [conf t autody day day time time \[-period days\]](#).

### **category-settings**

shows configuration settings for filter categories. Can be changed with [conf t category-settings](#).

### **clock**

shows timezone and daylight saving time settings. Can be changed with [conf t clock](#).

### **ddos**

shows the current ddos settings. Can be changed with [conf t ddos](#).

### **default-alert-sink**

shows the default email address that attack alerts will be directed to. Can be changed with [conf t default-alert-sink](#).

### **default-gateway**

shows the device default gateway. Can be changed with [conf t default-gateway ip](#).

### **dhcp-server**

shows the configuration of the DHCP server. Can be changed with [conf t dhcp-server](#).

### **dns**

shows the configuration of the DNS server.

### **email-rate-limit**

shows the maximum number of email notifications the system will send every minute. The minimum is 1; the maximum is 35. Can be changed with [conf t interface](#).

### **filter number**

shows the filter data for a specific filter. Can be changed with [conf t filter](#).

### **firewall**

shows firewall configurations.

### **alg**

shows the application layer gateway (ALG).

### **alg sip**

show the Session Initiation Protocol (SIP) sessions.

### **rule [id] [from src] [to dst]**

shows firewall rules. Enter a rule ID to display a single rule. The value of *src* or *dst* can be “this-device” to indicate the local device.

### **schedule**

shows firewall schedules.

### **service**

shows firewall services.

### **service-group**

shows firewall service groups.

### **virtual-servers**

shows firewall virtual servers.

### **high-availability**

shows the configuration for the transparent high-availability. Can be changed with [conf t high-availability](#).

### **host**

shows the host name and host location.

### **interface**

shows configuration of all ports if no further qualifiers (port type, slot number, port number) are entered. To view the settings for the interface configuration, enter **show conf int settings**. Can be changed with [conf t interface](#).



**TIP** You can use the abbreviation **show conf int**. Also, you can define an alias using the **alias** command.

### **ethernet [slot port]**

shows Ethernet port information. The command abbreviation is **show conf int eth**. Use the command without parameters to show the status of all Ethernet ports. Use with a slot number and port number, separated by spaces, to view the status of a single port.

### **mgmtEthernet**

shows Management Ethernet port information. The command abbreviation is **show conf int mgmt**.

**settings**

shows the persistent configuration settings for MDI-detection and the Ethernet polling interval setting.

**virtual**

shows settings for all virtual interfaces.

**log**

shows the persistent configuration of the audit log. Can be changed with [conf t log audit select](#).

**monitor**

shows the persistent configuration of monitor thresholds. Can be changed with [conf t monitor](#).

**nms**

shows the NMS settings for community string, IP address, and port. Can be changed with [conf t nms](#).

**notify-contacts**

shows the notification contacts. Can be changed with [conf t notify-contact contact-name agg-period](#).

**ntp**

shows the NTP configuration.

**port**

shows the port configuration.

**profile**

lists all profiles that have been configured on the device. To view an individual profile, use [show profile profile-name](#). To change a profile, use [conf t profile profile-name](#).

**protection-settings**

shows the commands for configuring the protection settings. Can be changed with [conf t protection-settings](#).

**ramdisk**

shows the persistent configuration of the RAM disk sync interval. Can be changed with [conf t ramdisk](#).

**remote-syslog**

shows the persistent configuration of the remote-syslog. Shows the destination IP address for remote logging. Can be changed with [conf t remote-syslog](#).

**routing**

shows routing configuration.

**multicast**

shows multicast routing configuration.

### server

shows the persistent configuration of ssh, telnet, http, and https servers on the device. Can be changed with [conf t server](#).

### service-access

shows whether service-access is enabled or not. Can be changed with [conf t service-access](#).

### session

shows default session timeout for all sessions. Can be changed with [conf t session](#).



**Note:** **show conf session** does not show session settings because session settings are not persistent. Use [show session](#) to view current session configuration.

### sms

shows if SMS is enabled (“sms” or “no sms”) and other SMS configuration information. Can be changed with [conf t sms](#).

### tse

shows the configuration for the Threat Suppression Engine (TSE). This information includes connection table timeout, asymmetric network setting, adaptive aggregation threshold, and adaptive filter mode.

### user [-details]

displays user options that can be read back in as commands. The command abbreviation is **show conf u**.

### vpn

shows VPN configuration. This is a recursive command that executes all the show configuration vpn commands below.

#### ike

shows IKE configuration.

#### ipsec [sa]

shows IPsec configuration. Use **show configuration vpn ipsec sa** to show the configuration of IPsec Security Association.

#### l2tp

shows L2TP configuration.

#### pptp

shows PPTP configuration.

### web-filtering

shows the configuration of web content filtering.

#### default-rule

shows the default rule.

**filter-action**

shows the filter actions.

**filter-service**

shows the configuration of the filtering service.

**manual-filter**

shows the configuration of the manual filter.

**zone**

shows the configuration for a Security Zone.

**Using show conf**

*show user  
options to be  
read in as  
commands*

Use **show conf user** to list the user options. For example:

```
hostname# show conf user
user options max-attempts 5
user options expire-period 90
user options expire-action expire
user options lockout-period 5
user options attempt-action lockout
user options security-level 2
```

**show default-alert-sink**

The **show default-alert-sink** command shows the email-to address, email-from address, SMTP server domain, SMTP server IP address, and aggregation period settings for email alerts.

**show default-gateway**

The **show default-gateway** command shows the IP address of the default gateway.

**show dhcp-server**

The **show dhcp-server** command shows details of the DHCP server.

```
hostname# show dhcp-server
Current Leases: 4
Available Leases: 49
```

| IP Address   | Host Name | MAC Address       | Type    | Expires |
|--------------|-----------|-------------------|---------|---------|
| 192.168.2.10 | fbsd6-1   | 02:00:00:80:18:01 | Dynamic | 56m54s  |
| 192.168.2.25 | fbsd6-9   | 02:00:00:80:18:09 | Dynamic | 1d23h   |
| 192.168.2.26 | fbsd6-8   | 02:00:00:80:18:08 | Dynamic | 1d23h   |
| 192.168.2.11 | fbsd6-0   | 02:00:00:80:18:00 | Dynamic | 56m51s  |

**show filter** *number*

The **show filter** command shows filter data for a specific filter. Specify the filter by number.

**show firewall monitor**

The **show firewall monitor** command shows data usage for clients, services, and Web sites.

**clients**

shows client data usage.

**services**

shows service data usage.

**websites**

shows Web site data usage.

**Using show firewall monitor**

*monitoring  
Web site data  
usage*

Use **show firewall monitor websites** to show data usage statistics from Web sites.

```
hostname# show firewall monitor websites
Bandwidth (KBytes)  Sessions      Name
-----
10503              13           www.example.com
5000               5            www.google.com
1050               1            downloads.microsoft.com
10                 1            www.kernel.org
```

**show firewall rules** [*from* source-IP] [*to* destination-IP]

The **show firewall rules** command shows the firewall rules that are currently in effect on the device. The rules list shows the rule number, the action that the rule takes, source and destination, service, and ELR. Use the **from** and **to** parameters to filter the table by IP address.

**counters**

shows the number of times that each Permit or Block firewall rule has been activated. This number appears in the **Counter** column at the end of each listing.

**show firewall sessions** [*from* source-IP] [*to* destination-IP]

The **show firewall sessions** command displays the firewall session table. The table lists each session's source and destination zone and IP address, as well as the time remaining before the session expires. Use the **from** and **to** parameters to filter the table by IP address.

## show health

The **show health** command shows memory, disk usage, temperature, and thresholds of the device. Use the show health command without parameters to see all health statistics, or with one of the parameters to see only memory or disk usage.

### disk-space

shows current disk space usage for the /boot, /log, /usr, and /opt disk partitions.



**Tip:** To reduce disk usage, do one of the following:

- reset logs using the [“log \[alert | audit | block | firewallblock | firewallsession | packet-trace | system | vpn\]” on page 32](#)
- delete old boot images using [“boot” on page 29](#)

### memory

shows current memory (RAM) usage.



**Tip:** To reduce memory usage, use the LSM to make the following filter adjustments:

- reduce the number of filters that use alerts
- increase aggregation periods for action sets that include alerts
- reduce the number of filter exceptions
- use more global filters and fewer segment-specific filters
- deactivate filters that do not apply to your network (for example: IIS filters are not relevant if you only have Apache servers).

### power-supply

shows the current health of the power supply. If any power supplies for a device are interrupted, the power supply monitor feature will log a critical message in the system log. This feature is available on the following models: 200, 400, 1200, 2400 and 600E, 1200E, 2400E, 5000E.

## Using show health

*show current  
memory use*

Use **show health memory** to show current memory use.

```
hostname# show health memory
Memory          :
Current: 38 percent in use
Health: Normal
```

**show high-availability**

The **show high-availability** command shows the status of failover high availability: active, disabled, or standby.

**show interface**

The **show interface** command shows port type and status information. Use **show interface** without any options to show all ports. Use the **ethernet**, **mgmtEthernet**, or **vnam** options to show types of ports or individual ports.

**ethernet [-details] [slot port]**

shows interface information for all Ethernet ports, all Ethernet ports in one slot, or a single Ethernet port.

**mgmtEthernet [-details]**

shows interface information about the Management Ethernet port.

**virtual [ [-details id] | [ gre | external | internal ] ]**

shows information about a virtual interface.

*show status of  
all interfaces*

Use **show interface** with no parameters to show status information for all interfaces.

```
hostname# show int
Slot/Port          1/1
Type               Ethernet
Internet Address   192.168.65.14
Subnet Mask        255.255.255.0
MAC Address        00:80:42:11:9E:BC
MTU                1500
Link               up(1)
Speed              100
RX Unicast Pkts    941
RX Non-Unicast Pkts 3843
RX Error Pkts      0
RX Discards        0
RX Unknown Protocols 0
RX Total Pkts      4784
TX Unicast Pkts    1384
TX Non-Unicast Pkts 2
TX Total Pkts      1386
```

```
Slot/Port          7/1
Type               Ethernet
MTU                1500
Link               up(1)
Speed              1000
Duplex             Full(3)
RX Unicast Pkts    10
RX Multicast Pkts  0
RX Broadcast Pkts  385
RX Error Pkts      0
RX Discards        0
RX Unknown Protocols 0
RX Total Pkts      395
```

```

TX Unicast Pkts      0
TX Multicast Pkts    0
TX Broadcast Pkts    0
TX Total Pkts        0

```

```

Slot/Port      7/2
Type           GigabitEthernet
MTU            1500
Link           down(2)
Speed          1000
Duplex         Half(2)
RX Unicast Pkts      0
RX Multicast Pkts    0
RX Broadcast Pkts    0
RX Error Pkts        0
RX Discards         0
RX Unknown Protocols 0
RX Total Pkts        0
TX Unicast Pkts      0
TX Multicast Pkts    0
TX Broadcast Pkts    0
TX Total Pkts        0

```

```

Slot/Port      7/1
Type           VNAME
Internet Address 0.0.0.0
Subnet Mask      0.0.0.0
MAC Address      00:07:99:00:06:42
Link            down(2)

```

```

Slot/Port      7/2
Type           VNAME
Internet Address 0.0.0.0
Subnet Mask      0.0.0.0
MAC Address      00:07:99:00:06:42
Link            down(2)

```

*show status of  
a Ethernet  
port*

Use **show interface ethernet slot port** to show the status of a Ethernet port.

```

hostname# show int eth 6 1
Slot/Port: 6/1
Type: Ethernet
MTU            1500
Speed          1000
Duplex         ?
Link           up(1)
RX Unicast Pkts      0
RX Multicast Pkts    0
RX Broadcast Pkts    0
RX Error Pkts        0
RX Discards         0
RX Unknown Protocols 0
RX Total Pkts        0
TX Unicast Pkts      0
TX Multicast Pkts    0
TX Broadcast Pkts    0
TX Total Pkts        0

```

*show status of  
a mgmt  
Ethernet port*

Use **show interface mgmtEthernet** to show the status of the Management Ethernet port.

```
hostname# show int mgmt
Slot/Port          1/1
Type                Ethernet
Internet Address    192.168.65.14
Subnet Mask         255.255.255.0
MAC Address         00:80:42:11:9E:BC
MTU                 1500
Link                up(1)
Speed               100
RX Unicast Pkts     941
RX Non-Unicast Pkts 3844
RX Error Pkts       0
RX Discards         0
RX Unknown Protocols 0
RX Total Pkts       4785
TX Unicast Pkts     1384
TX Non-Unicast Pkts 2
TX Total Pkts       1386
```

### show local-user

The **show local-user** command lists the local users that are defined on the device and the privilege groups to which they are assigned.

#### sessions

lists local user sessions.

*show local  
users*

Use **show local-user** to show local users and their privilege groups.

```
hostname# show local-user

Name                               Privilege Group
-----
bar                                Allow_VPN_access
foo                                Allow_VPN_access
```

*show local  
user sessions*

Use **show local-user sessions** to show local users, their privilege groups, and their sessions.

```
hostname# show local-user sessions

Name           Privilege Group   IP Address      Logged In
-----
test           RADIUS            192.204.181.137 00:15:40
```

### show log

The **show log** command shows log file listings from the audit, fault, policy, peer-to-peer, and system logs. You must provide a log name when you use the show log command.



**Note:** When you view the audit log, the user listed for the logged events may include SMS, LSM, and CLI. The audit log displays both who performed an action (user name) and where they logged in from (such as WEB and CLI.). The audit log is the only log that displays this information.

### Common show log command flags

The different X family logs have a number of command flags that are common to all logs.

#### **-c**

clears the screen before displaying log entries.

#### **-end-time** < yyyyymmdd | hh:mm:ss | "yyyyymmdd hh:mm:ss">

filters out log entries timestamped after *yyyyymmdd*, *hh:mm:ss*, or *"yyyyymmdd hh:mm:ss"*.

#### **-match**

shows only those log entries that match a specified pattern, similar to a file grep.

#### **-max-records** <1-65535>

shows the first 1 to 65535 records in the log.

#### **-n** <10-128>

shows 10 to 128 log entries at a time.

#### **-start-time** < yyyyymmdd | hh:mm:ss | "yyyyymmdd hh:mm:ss">

filters out log entries timestamped before *yyyyymmdd*, *hh:mm:ss*, or *"yyyyymmdd hh:mm:ss"*.

#### **-tail**

shows the last **-n** records in the log.



**Note:** The **-tail** flag cannot be used with the **-severity flag**, nor can it be used with the **-<module-name>** flag

#### **-width** <38-256>

width of output.

### alert

displays alert log entries. Alert log entries include date/time, policy name, vulnerability filter name, service, source address, and destination address information about network traffic that has triggered filters.

#### **-module** *module-name*

displays records according to the module name. Refer to the log entries for module names.

### audit

displays audit log entries. Audit log entries include date, time, access method, audit action, source IP address, access role, login name, action outcome [pass/fail], and action attempted.

#### **-user** "login-name"

displays log entries relating to the specified login name.

### **-status < PASS | FAIL >**

displays only records with pass or fail status.

### **-ip ip**

displays log records reflecting access from the specified IP address

### **[WEB,CLI,SNMP,OTHER]**

displays records based on the interface through which the device was accessed.

### **block**

displays block log entries. Block log entries include date/time, policy name, vulnerability filter name, service, source address, and destination address information about network traffic that has triggered and been blocked by filters.

### **-module module-name**

displays records according to the module name. Refer to the log entries for module names.

### **firewallblock**

displays a log of all firewall block actions.

### **-module module-name**

displays records according to the module name. Refer to the log entries for module names.

### **-loglevel [ CRIT | ERR | WARN | INFO | OTHER ]**

displays records according to the log level.

### **firewallsession**

displays a log of all firewall sessions.

### **-module module-name**

displays records according to the module name. Refer to the log entries for module names.

### **-loglevel [ CRIT | ERR | WARN | INFO | OTHER ]**

displays records according to the log level.

### **system**

displays entries from the system log. System log entries show the date, time, entry severity, entry author component, and log message.

### **-module module-name**

displays records according to the module name. Refer to the log entries for module names.

### **-loglevel [ CRIT | ERR | WARN | INFO | OTHER ]**

displays records according to the log level.

**vpn**

displays a log of VPN sessions, events, and alerts.

**-module** *module-name*

displays records according to the module name. Refer to the log entries for module names.

**-loglevel** [ **CRIT** | **ERR** | **WARN** | **INFO** | **OTHER** ]

displays records according to the log level.

---

**show mfg-info**

The **show mfg-info** command displays the serial number, model number, MAC address, and other manufacturing information for the device.

---

**show np**

The **show np** command displays various network processor statistic sets. These commands should be used for support and debugging purposes only. They do not convey useful information for most users.

**engine**

displays information about packet processing.

**filter**

displays the packets that have been filtered and the reasons for the filter actions. The command also displays the packets that had protocol level errors on a per-error basis.

**packet**

displays general packet statistics, including the total number of packets sent and received and per-second packet profiling.

**parse**

displays the total number of packets of known protocols, unknown protocols, and how many packets could be parsed or not parsed.

**rule**

displays statistics related to rules and the number of rules that have been created or deleted. The command also displays a breakdown of rules by type.

**fpp**

displays Fast Pattern Processor statistics.

**general statistics**

displays the network processor general statistics information and includes incoming, outgoing and congestion information.

**linx**

displays pattern match statistics.

### **protocol-mix**

displays protocol specific statistics broken down by layer.

### **reassemble**

displays the specified reassembly statistics.

### **ip**

displays the IP reassembly statistics.

### **tcp**

displays the tcp reassembly statistics.

### **rsp**

displays the Routing Switch Processor statistics.

### **rule-stats**

displays the top 20 filters and associated success rates.

### **softlinx**

displays statistical data for internal hardware/software engines.

**tier-stats**

displays general statistics with percentages for tier performance.

- Tier 1 — Hardware tier. The ratio displays the amount of traffic directed at the management processor.
- Tier 2 — PCI bus to the management CPU. The ratio displays the percentage of data that passed soft lnx.
- Tier 3 — Management CPU. The ratio displays the percentage of traffic that is actionable.

**xslcounters values**

displays the persistent values for the network processor xslcounters. The command displays 1 entry for most devices and following information:

- slot: The slot the XSL is in
- timestamp: The timestamp (in kernel ticks) when the XSL counters were read
- synCount: The 32-bit counter, incremented each time a TCP SYN packet is received
- estCount: The 32-bit counter, incremented each time a TCP flow completes the 3-way handshake successfully
- activeCount: The 32-bit counter, incremented each time a TCP flow in the XSL connection table moves past the ESTABLISHED state into the
- ACTIVE state: The state of the xslcounter. ACTIVE is when data flows on the TCP connection after the 3-way handshake was completed.

**Using show np**

*show np  
engine packet  
screeningfilter  
statistics*

Use **show np engine** with the **filter** parameter to view the network processor packet screening filter statistics.

```
hostname# show np engine filter
```

```
Packet Screening Filter Statistics:
```

```
-----
```

```
Total packets filtered      = 0
Packets accepted            = 0
Packets accepted w/error    = 0
Packets denied              = 0
Packets fwd to reassembly   = 0
Packets failed reassembly   = 0
Packets denied by CT        = 0
UDP packets without cksum   = 0
Pkts fwd to TCP reassembly  = 0
```

```
Bad IP version              = 0
Bad IP hdr len              = 0
Bad IP ttl                  = 0
Bad IP total len            = 0
Bad IP fragment             = 0
IP fragment                 = 0
Bad TCP hdr len             = 0
Bad TCP rsvd bits           = 0
Bad TCP total Len           = 0
```

```
Bad TCP flags           = 0
Bad UDP total len       = 0
Bad ICMP total len      = 0
Bad ARP addr type       = 0
Bad ARP addr len        = 0
```

### *show np engine packet statistics*

Use **show np engine** with the **packet** parameter to view the network processor packet statistics.

```
hostname# show np engine packet
```

```
Packet Statistics:
```

```
-----
```

```
PCB alloc count:        = 0
PCB free count:         = 0
```

```
Rx packets OK           = 0
Rx packets dropped       = 0
Rx packets dropped no pcb = 0
Rx packets dropped rx err = 0
```

```
Tx packets OK           = 0
Tx packets discarded     = 0
Tx packets discarded tx err = 0
```

```
Rx bytes OK             = 0
Tx bytes OK              = 0
```

```
Rx due to cross pkt match = 0 ( 0%)
Rx due to TCP seq         = 0 ( 0%)
Rx due to reroute         = 0 ( 0%)
Rx due to trigger         = 0 ( 0%)
Rx due to dest ID host    = 0 ( 0%)
Rx due to dest ID static ee = 0 ( 0%)
Rx due to dest ID dyn ee  = 0 ( 0%)
```

```
Per Second Statistics:
```

```
Bytes per second         = 0
Max bytes per second     = 0
Min bytes per second     = 0
Average packet size      = 0
Packets per second       = 0
Max packets per second   = 0
Min packets per second   = 0
```

*show np  
engine parser  
statistics*

Use **show np engine** with the **parse** parameter to view the network processor parser statistics.

```
hostname# show np engine parse
```

```
Parser Statistics:
-----
Total packets           = 0
Parseable packets      = 0
Unparseable packets    = 0
Unknown packets        = 0
Unknown L3 packets     = 0
IP packets              = 0
  Fragments             = 0
  TCP packets           = 0
  UDP packets           = 0
  ICMP packets          = 0
  Unknown IP packets    = 0
ARP request packets    = 0
ARP reply packets      = 0
RARP requests          = 0
RARP replies           = 0
```

*show np  
engine rule  
statistics*

Use **show np engine** with the **rule** parameter to view the network processor rule statistics.

```
hostname# show np engine rule
```

```
Rule Statistics:
-----
Rule hits                = 0
Rule misses              = 0
Rules created            = 4888
Rules deleted            = 3258

Function Call Counters:
Create called            = 4888
Delete called            = 3258
Compressed rules         = 1482
Early exit rules         = 46
FPP rules                = 102
FPP total removes        = 506
FPP total adds           = 608
Linux rules              = 1566
Total rules              = 1630
```

*show np fast  
pattern  
processor  
statistics*

Use **show np** with the **fpp** parameter to view the network processor fast pattern processor statistics.

```
hostname# show np fpp

FPP Statistics:
-----

FPP General Statistics:
No timedout PDUs          = 0
No oversize PDUs          = 0
No ready queue overflows  = 0

FPP Memory Usage Statistics:
Memory used               = 1138176
Flow memory used          = 842
X8s used                  = 17272
X8s free                  = 1127
X2s used                  = 410
X2s free                  = 38
X1s used                  = 128
X1s used                  = 128

FPP Tree 0 Statistics:
Memory used               = 88
No learns                 = 1
No unlearns               = 0
No writes                 = 12
```

*show np  
general  
statistics*

Use **show np general statistics** to view the network processor general statistics.

```
hostname# show np general statistics

General Statistics:
-----

Incoming                  =          0
Outgoing                  =          0
Congestion                =          0
Deep                     =          0
Matched                   =          0
Blocked                   =          0
```

*show np linx  
statistics*

Use **show np linx** to view the network processor linx statistics.

```
hostname# show np linx

Pattern Match Statistics:
-----

String size --->      5,      8,     12
Class 0 count =      0,      0,      0
Class 1 count =      0,      0,      0
Class 2 count =      0,      0,      0
Class 3 count =      0,      0,      0
Class 4 count =      0,      0,      0
Class 5 count =      0,      0,      0
Class 6 count =      0,      0,      0
Class 7 count =      0,      0,      0
Class 8 count =      0,      0,      0
Class 9 count =      0,      0,      0
Class 10 count =     0,      0,      0
Class 11 count =     0,      0,      0

Did changed count              =      0
Did changed TCP count          =      0
Did changed reroute count      =      0
Did changed bad sequence count =      0
```

*show np  
protocol  
specific  
statistics*

Use **show np protocol-mix** to view the network processor protocol-specific statistics.

```
hostname# show np prot

Protocol-Specific Statistics:
-----

General:
PDUs received      = 0
Discard            = 0
Hdr cksum discard  = 0
Proto cksum discard = 0
All cksum discard  = 0

Ethernet:
Ethernet IPX       = 0
Ethernet ARP       = 0
Ethernet SNAP      = 0
Ethernet IPV4 other = 0
Ethernet IPV4 TCP   = 0
Ethernet IPV4 UDP   = 0
Ethernet IPV4 ICMP  = 0
Ethernet other     = 0

VLAN:
VLAN IPX           = 0
VLAN ARP           = 0
VLAN Ethernet other = 0
VLAN IPV4 other    = 0
VLAN IPV4 TCP      = 0
VLAN IPV4 UDP      = 0
VLAN IPV4 ICMP     = 0

Non Standard:
Not IPV4           = 0
IPHL not equal 5   = 0
```

```
Frag 001          = 0
Frag 011          = 0
Frag 100          = 0
Frag 101          = 0
Frag 111          = 0
Frag OFS          = 0
Same IP addr      = 0
Same port         = 0
TCP DLEN          = 0
```

*show np ip  
reassembly  
statistics*

Use **show np reas ip** to view the network processor IP (internet protocol) reassembly statistics.

```
hostname# show np reas ip

IP Reassembly Statistics:
-----

Reassembly queues contain    0 frags in    0 dgrams

Summary:
Fragments incoming          = 0
Fragments kept              = 0
Fragments dropped (duplicate) = 0
Fragments dropped (other)   = 0
Dgrams completed            = 0
Dgrams dropped               = 0
Dgrams frag overlap         = 0
Dgrams outgoing             = 0

Reasons for dropping:
Misleading MF bit           = 0
Exceeded frag limit         = 0
Exceeded dgram limit        = 0
No mem for frag              = 0
No mem for dgram            = 0
Expired frags                = 0
Frag len / total len mismatch = 0
Frag out of range           = 0
Frag len not multiple of 8   = 0
Bugs (should all be zero):
Null PCB                    = 0
Not IPV4                     = 0
Not a fragment               = 0
Invalid hdr len in pullup    = 0
Invalid pld len in pullup    = 0
No first frag in pullup      = 0
No last frag in pullup       = 0
Invalid size                  = 0
```

*show np  
reassembly tcp  
statistics*

Use **show np reas tcp** to view the network processor reassembly tcp statistics.

```
hostname# show np reas tcp

TCP Reassembly Statistics:
-----

TCP reassembly queues contain    0 frags    0 flows    0 linx entries
Total bytes allocated 27926528

Summary:
Fragments incoming          = 0
Flows given up              = 0
Flows dropped                = 0
Flows outgoing              = 0
```

```

Flows pulled up                = 0
Flows max active               = 0
Fragments max active          = 0

Reasons for Dropping Flow:
Could not allocate flow        = 0
No mem for flow                = 0
Expired flows due to old age   = 0
Expired flows due to early retirement = 0
Expired frags due to old age   = 0
Found missing sequence        = 0
Saw pre-sequence              = 0
Matched category              = 0
Bypass/throttle on            = 0

Reasons for Returning:
Bad TCP checksum               = 0
TTL too small                  = 0
TCP resend                     = 0
No trigger                     = 0
Reroute w/o flow (orphan)     = 0

Miscellaneous:
Stop reroute called           = 0
Longest flow linked list      = 0
Longest linx linked list      = 0

Bugs (should all be zero):
Null PCB                      = 0
Not IPV4                      = 0
Not TCP                       = 0
Invalid hdr len in pullup     = 0
Exceeded buffer size in pullup = 0
Could not find or create flow  = 0
Could not alloc linx entry     = 0
Total length exceeded max data size = 0

```

*show np  
routing switch  
processor  
statistics*

Use **show np rsp** to view the network processor routing switch processor statistics.

```
hostname# show np rsp
```

```
RSP Statistics:
-----
```

```

RSP General Statistics:
Total memory blocks      = 524288
Used memory blocks       = 0
PDUs passed              = 0
PDUs passed tagged 0     = 0
PDUs passed tagged 1     = 0
PDUs passed tagged 2     = 0
PDUs passed tagged 3     = 0
PDUs passed tagged 4     = 0
PDUs passed tagged 5     = 0
PDUs passed tagged 6     = 0
PDUs passed tagged 7     = 0
PDUs discarded FPL       = 0
PDUs discarded TM param 00 = 0
PDUs discarded TM param 01 = 0
PDUs discarded QI deq zero = 0
TTT passed TM            = 0
TTT discarded TM         = 0
Blocks passed TM         = 0
Blocks discarded TM       = 0

```

Blocks discarded ROB = 0

RSP LPORTs and Schedulers:

|           | blksLeft | pdusPassd | tttsPassd | pdusDiscrd | tttsDiscrd | tttThresh |
|-----------|----------|-----------|-----------|------------|------------|-----------|
| LPORT 0:  | 0        | 0         | 0         | 0          | 0          | 0         |
| SCH 0:    | 0        | 0         | 0         | 0          | 0          | -         |
| LPORT 31: | 0        | 0         | 0         | 0          | 0          | 0         |
| SCH 0:    | 0        | 0         | 0         | 0          | 0          | -         |

*show np tier-  
stats*

Use **show np tier-stats** to view the tier statistics.

```
hostname# show np tier-stats
Tier 1:
  Receive  Mbps      = 56
  Transmit  Mbps      = 56
  Receive  pkts/sec   = 14268
  Maximum  pkts/sec   = 27355
  Bytes/packet avg    = 494
  Utilization          = 3 %
  Ratio to next tier   = 62.41 %

Tier 2:
  Utilization          = 6 %
  Ratio to next tier   = 99.86 %

Tier 3:
  Receive  Mbps      = 35
  Transmit  Mbps      = 35
  Receive  pkts/sec   = 5210
  Maximum  pkts/sec   = 12544
  Bytes/packet avg    = 845
  Utilization          = 33 %
  Ratio to next tier   = 40.36 %
```

*show np rule-  
stats*

Use **show np rule-stats** to view the rule statistics.

```
hostname# show np rule-stats
  Filter  Flows  Success  % Total  % Success
  -----
    2310   96449         0        21         0.00
    1259   54516    54008        12        99.06
    1044   18475         0         4         0.00
    2384   15459         0         3         0.00
    2385   15459         0         3         0.00
    1925   15459         0         3         0.00
    1647   15459         0         3         0.00
    2388   15459         0         3         0.00
    1924   15459         0         3         0.00
    1648   15459     149         3         0.96
    1923   15459         0         3         0.00
    2227   15437         0         3         0.00
    1650   15405         0         3         0.00
    1047   14372         0         3         0.00
    1645   13743         0         3         0.00
    2541   11654         0         2         0.00
    2644   11647         0         2         0.00
     906    7312         0         1         0.00
    1117    6302         0         1         0.00
    2860    5996         0         1         0.00
Total of 453572 flows
```

### *show np xslcounters values*

Use **show np xslcounters values** to view the network processor xslcounter values.

```
hostname# show np xslcounters values
Slot    timestamp    synCount    estCount    activeCount
-----
3        5946554          0           0           0
```

### **show ntp**

Use **show ntp** to view the current NTP status. You must use this command with one of the following subcommands.

#### **sessions**

displays information about the current NTP session.

#### **status**

displays the current clock and NTP status.

### **Using show ntp**

### *show current ntp settings*

To show the current NTP settings, use the **show ntp status** command. For example:

```
hostname# show ntp status
clock status: Synchronized
clock stratum: 4
reference clock ID: 10.0.1.100
root delay: 0.0032
root dispersion: 8.0194
clock precision: 2^-6
NTP reference clock: 16:59:33.396 UTC Feb 19 2007 (45D9D775.17A2FD88)
Current system time: 16:59:33.399 UTC Feb 19 2007 (45D9D775.17D07E3F)
```

### **show policy counters**

shows the Total, Invalid, Alerted, and Blocked counters



**Note:** Packet counters provide a snapshot look at traffic through your network. Counters are not synchronized with each other, and packets may be counted more than once in some situations.

### **show profile** profile-name

The **show profile** command displays the policies, security zone pairs, category settings, and protection limits defined for the named profile.

### **show protection-settings**

The **show protection-settings** command displays the configured exceptions and apply-only rules restrictions for Application Protection, Infrastructure Protection, and Performance Protection filters.

show ramdisk

The **show ramdisk** command displays information on the RAM disk of the device.

files

shows the RAM disk files and sizes.

stats

shows the statistics of RAM disk size and usage, the sync interval countdown, and information regarding log files stored on the RAM.

Using show ramdisk

show RAM  
disk files

Use **show ramdisk files** to view the current files and file sizes for RAM disk.

```
hostname# ramdisk files
-----
/ramLog filesystem: Size=40,089,600   Inuse=75,776   Free=40,013,824
Monitored files:
 19596 /ramLog/log/sys/message.log      3766 /log/sys/message.log.z
    0 /ramLog/log/sys/message.log.1      0 /log/sys/message.log.1.z
 11938 /ramLog/log/audit/audit.log      2671 /log/audit/audit.log.z
    0 /ramLog/log/audit/audit.log.1      0 /log/audit/audit.log.1.z
 30812 /ramLog/log/block/block.log      0 /log/block/block.log.z
    0 /ramLog/log/block/block.log.1      0 /log/block/block.log.1.z
 2382 /ramLog/log/alert/alert.log      0 /log/alert/alert.log.z
    0 /ramLog/log/alert/alert.log.1      0 /log/alert/alert.log.1.z
    0 /ramLog/log/peer/peer.log      0 /log/peer/peer.log.z
    0 /ramLog/log/peer/peer.log.1      0 /log/peer/peer.log.1.z
-----
/ramRO filesystem: Size=8,340,480   Inuse=6,511,616   Free=1,828,864
No monitored files - Read-only
-----
/ramTmp filesystem: Size=12,518,400   Inuse=11,264   Free=12,507,136
No monitored files - Read-only
```

show current  
RAM disk  
stats

To show the current statistics for RAM disk usage of logs, use the **show ramdisk stats** command. For example:

```
hostname# show ramdisk stats
Enabled:      TRUE
Sync Delay:   1 secs   forced sync:   28
Sem Write Timeout: 5 secs   error cnt:   0
Write Error Count: 0 (total)
Write Error Count: 0 (consecutive) (allowed=3)

RAM Disk Stats - Begin: 2004-05-02 11:07:37 [CST]
                  End: 2004-05-03 08:36:59 [CST]

--- RAM Disk - /ramLog -----
Alloc Sz:      40262144
File Count:    10

   File                      Interval Cntdwn Dirty   Flush   Sync   F/Sync   F/min   S/min
/ramLog/log/sys/message.log    30    13  FALSE    30     25    1.20    0.02    0.02
/ramLog/log/sys/message.log.1  30    12  FALSE     0     13    0.00    0.00    0.01
```

```

/ramLog/log/audit/audit.log      30    11    FALSE    37      21      1.76    0.03    0.02
/ramLog/log/audit/audit.log.1    30    10    FALSE     0       1      0.00    0.00    0.00
/ramLog/log/block/block.log      -1     0     TRUE    73       0      0.00    0.06    0.00
/ramLog/log/block/block.log.1    -1     0    FALSE     0       0      0.00    0.00    0.00
/ramLog/log/alert/alert.log      -1     0     TRUE     2       0      0.00    0.00    0.00
/ramLog/log/alert/alert.log.1    -1     0    FALSE     0       0      0.00    0.00    0.00
/ramLog/log/peer/peer.log        -1     0    FALSE     0       0      0.00    0.00    0.00
/ramLog/log/peer/peer.log.1      -1     0    FALSE     0       0      0.00    0.00    0.00
-----

```

### show rate-limit-speeds

The **show rate-limit-speeds** command lists the rate limit speeds, in Kbps, that are valid on the device.

### show routing

The show routing commands below show the details of routing on the device.

#### multicast

shows multicast groups.

#### static-routes

shows the static routes.

#### statistics

shows the routing statistics.

#### table [ip ip netmask mask]

shows the routing table.

### Using show routing

*show  
multicast  
groups*

Use **show routing multicast** to view multicast groups.

```

hostname# show routing multicast
IGMP Querier Status

```

| Interface | IP Address     | Querier       | Groups    |
|-----------|----------------|---------------|-----------|
| 1         | 192.168.1.254  | 192.168.1.254 | 225.1.1.1 |
| 2         | 192.168.2.254  | 192.168.2.10  | 227.1.1.1 |
| 3         | 10.245.230.239 |               |           |

*show static  
routes*

Use **show routing static-routes** to view static routes.

```

hostname# show routing static-routes
Destination      Subnet Mask      Gateway           Metric
-----
0.0.0.0          0.0.0.0          10.245.230.225    1
10.0.0.0         255.0.0.0        10.245.230.245    1

```

*show routing  
table*

Use **show routing table** to view the routing table.

```
hostname# show routing table
Destination      Subnet Mask      Nexthop          Metric   Age      Status
-----
127.0.0.0        255.0.0.0        127.0.0.1        1        -        Local
192.168.1.0      255.255.255.0    192.168.1.254    1        -        Direct
192.168.2.0      255.255.255.0    192.168.2.254    1        -        Direct
10.245.230.224   255.255.255.224  10.245.230.239   1        -        Direct
Default          0.0.0.0          10.245.230.225   1        -        Static
10.245.230.239   255.255.255.255  127.0.0.1        1        -        Local
192.168.1.254    255.255.255.255  127.0.0.1        1        -        Local
192.168.2.254    255.255.255.255  127.0.0.1        1        -        Local
255.255.255.255  255.255.255.255  192.168.1.254    1        -        Direct
255.255.255.255  255.255.255.255  192.168.2.254    1        -        Direct
```

### show server

The **show server** command shows what servers are running on the device.

*show what  
servers are  
currently  
running*

```
hostname# show server
      ssh: Running
      http: Disabled
      https: Running
  browser-check: Running
```

### show service-access

The **show service-access** command shows whether service access is enabled or disabled. Service access is enabled with [conf t service-access](#).

*show service  
access status*

```
hostname# show service-access
Service-Access is disabled.
```

### show session

The **show session** command shows session configurable parameters.

*show current  
terminal  
session  
settings*

```
hostname# show session
Current Session Settings
Terminal Type      = vt100
Screen width       = 80
Screen height      = 24
Hard wrap          = Disabled
More               = Disabled
Session Timeout    = 20
```

**show sms**

The **show sms** command indicates if the device is under the control of an SMS. If it is under SMS control, it displays the SMS IP address.

*show sms  
status*

```
hostname# show sms
Device is not under SMS control.
```

**show timezones**

The **show timezones** command lists all time zones that can be used when configuring the system clock.

*show  
timezone  
abbreviations*

```
hostname# show timezones
ZONE   OFFSET   MIN   DST   Notes
-----
ACST    +9:30    -570  OFF   (AU Central Standard Time)
AEST    +10:00   -600  OFF   (AU Eastern Standard/Summer Time)
AKST    -9:00     540  OFF   (Alaska Standard Time)
AST     -4:00     240  OFF   (Atlantic Standard Time)
AWST    +8:00    -480  OFF   (AU Western Standard Time)
CET     +1:00    -60  OFF   (Central Europe Time)
CST     -6:00     360  OFF   (Central Standard Time)
EET     +2:00    -120  OFF   (Eastern Europe Time)
EST     -5:00     300  OFF   (Eastern Standard Time)
GMT      0:00      0  OFF   (Greenwich Mean Time)
HST    -10:00     600  OFF   (Hawaiian Standard Time)
JST     +9:00    -540  OFF   (Japan Standard Time)
KST     +9:00    -540  OFF   (Korea Standard Time)
MSK     +3:00    -180  OFF   (Moscow Time)
MST     -7:00     420  OFF   (Mountain Standard Time)
NZST    +12:00   -720  OFF   (New Zealand Standard Time)
PST     -8:00     480  OFF   (Pacific Standard Time)
WET      0:00      0  OFF   (Western Europe Time)
GMT-12  -12:00    720  OFF   (Time zone GMT-12)
GMT-11  -11:00    660  OFF   (Time zone GMT-11)
GMT-10  -10:00    600  OFF   (Time zone GMT-10)
GMT-9   -9:00     540  OFF   (Time zone GMT-9)
GMT-8   -8:00     480  OFF   (Time zone GMT-8)
GMT-7   -7:00     420  OFF   (Time zone GMT-7)
GMT-6   -6:00     360  OFF   (Time zone GMT-6)
GMT-5   -5:00     300  OFF   (Time zone GMT-5)
GMT-4   -4:00     240  OFF   (Time zone GMT-4)
GMT-3   -3:00     180  OFF   (Time zone GMT-3)
GMT-2   -2:00     120  OFF   (Time zone GMT-2)
GMT-1   -1:00      60  OFF   (Time zone GMT-1)
GMT+1    +1:00    -60  OFF   (Time zone GMT+1)
GMT+2    +2:00   -120  OFF   (Time zone GMT+2)
GMT+3    +3:00   -180  OFF   (Time zone GMT+3)
GMT+4    +4:00   -240  OFF   (Time zone GMT+4)
GMT+5    +5:00   -300  OFF   (Time zone GMT+5)
GMT+6    +6:00   -360  OFF   (Time zone GMT+6)
GMT+7    +7:00   -420  OFF   (Time zone GMT+7)
GMT+8    +8:00   -480  OFF   (Time zone GMT+8)
GMT+9    +9:00   -540  OFF   (Time zone GMT+9)
GMT+10   +10:00  -600  OFF   (Time zone GMT+10)
GMT+11   +11:00  -660  OFF   (Time zone GMT+11)
GMT+12   +12:00  -720  OFF   (Time zone GMT+12)
```

**show tse**

The **show tse** command displays information about the Threat Suppression Engine.

**adaptive-filter top-ten**

displays the top ten adaptive filters that are currently in use to reduce congestion on the Threat Suppression Engine (TSE).

**connection-table**

displays the connection-table information for the Threat Suppression Engine (TSE).

**blocks**

displays the blocked streams in the connection table.

**timeout**

displays the global timeout setting for the connection table.

**rate-limit streams**

displays the rate-limited streams in the connection table. You can use the [“rate-limit streams” on page 32](#) command to clear the streams.

**show user [-details]**

The **show user** command shows all administrator-user login accounts on the X Family and the level of username and password security checking that is enabled.

Using the command with the **-details** flag includes the information about the maximum number of login attempts and remaining time the account will be locked out, if applicable.

**Using show user**

*show the users  
and their  
options*

Use **show user** to view the user accounts on the system.

```
hostname# show user
Total Users: 2
```

| User Name | Access Role | Last Password Update | State   |
|-----------|-------------|----------------------|---------|
| admin     | super-user  | 2003-08-07 19:23:19  | Enabled |
| su        | super-user  | 2003-08-13 18:44:19  | Enabled |

*show the user  
options and  
security level  
details*

Use **show user -details** to view the user account details.

```
hostname# show user -details
Total Users: 1
```

| User Name | Access Role | Last Password Update | State | Attempts | Lockout Until |
|-----------|-------------|----------------------|-------|----------|---------------|
|-----------|-------------|----------------------|-------|----------|---------------|

```
-----
admin                               super-user    2003-08-28 13:39:10  Enabled      0 -
-----
```

### show version

The **show version** command displays the version of the device, the serial number, and the vulnerability filter package that is currently running. It also lists the model that you have, when it was last booted, and how long it has been running since the last boot.

*show device  
software and  
versions*

```
hostname# show version
      Serial: X-X5-Generic-0005
      Software: 2.5.0.6642  Build Date: "Jun 12 2006, 09:26:05" Production
      Digital Vaccine: 2.5.0.6632
      Model: X5
      Product Code: 3CRTPX5-73
      Host Board: t10t
      Rev: A

      Encryption: 256 bit

System Boot Time: 2006-06-14 10:48:55 CST
Uptime is 2 hours, 38 minutes, 47 seconds
```

### show vpn

Use the **show vpn** commands to view information about VPN connections.

#### ipsec

shows IPsec connections.

*show IPsec  
connections*

```
hostname# show vpn ipsec
Name      Peer      Local ID      Peer ID      Status
-----
test      10.245.230.240  10.245.230.230  10.245.230.240  Phase 1 idle
           192.168.3.0/24  192.168.1.0/24
test2     10.245.230.239  10.245.230.230  10.245.230.239  Phase 1 up
           192.168.3.0/24  192.168.2.0/24  Phase 2 up
```

#### l2tp [-details < remote-ip ip | username name | remote-ip ip username name >]

shows L2TP connections.

*show L2TP  
connections*

```
hostname# show vpn l2tp
L2TP Tunnel IP Remote IP      Username      Status
-----
192.168.5.19  10.0.5.200    test         Up
```

#### pptp [-details < remote-ip ip | username name | remote-ip ip username name >]

shows PPTP connections.

*show PPTP  
connections*

```
hostname# show vpn pptp -details username steve
PPTP Tunnel IP: 192.168.5.16  Hostname: local
Remote Ip:      10.0.5.200    Username:  steve
PPP Auth:       MSCHAP2      Encryption: yes  Keylength: 40 Bits
Bytes Sent:     0             MTU:          1000
Bytes Received: 72            MRU:          1500
```

Logged In: 0:00:55

---

### **show web-filter category** [url]

Use the **show web-filter category** command to show the filtering categories. Enter a specific URL to see what category it falls under.

*show Web  
filter category*

```
hostname# show web-filter category www.google.com  
'www.google.com' belongs to category: Search Engines
```

---

## **snapshot**

access: global; super-user, admin

The **snapshot** command creates and manages snapshots of the system's configuration settings. These snapshots can be applied to multiple systems, used to roll back to previously saved settings, and to make a backup of your current settings.

---

### **create** name

creates a snapshot of the system with the specified name.

---

### **list**

displays a list of available snapshots.

---

### **remove** name

deletes the snapshot by name.

---

### **restore** name

replaces current settings on the system with the settings in the named snapshot. The restore process may take time and will require restart of the device when complete.

---

## **traceroute**

access: global; all

The **traceroute** command sends a packet between a source and destination address and displays the route that the packet took and the number of hops.

ip

IP address of the destination.

**-F**

specifies that the packet not be fragmented. This stops the traceroute from being fragmented as it is passed through various routes, allowing you to calculate the maximum MTU size.



**Note:** This option is not supported when performing a UDP traceroute.

**-f**

sets the starting TTL.

**-I**

specifies ICMP ECHO instead of UDP probe.

**-m**

specifies the maximum number of hops.

**-n**

prints hop addresses numerically.

**-p**

sets the base UDP port.

**-Q**

stops traceroute from probing the hop after the maximum timeout.

**-q**

sets the number of probe queries.

**-w**

specifies the maximum time, in seconds, to wait for a probe response.

## traffic-capture

access: global, all

The **traffic-capture** command captures packet traces of monitored traffic management encountered by the device.

---

### export

exports a captured data stream.

**host**

the IP address to which you want to export the data stream.

**destination**

the destination directory on the target system to which the data stream will be saved.

### **file**

the name of the file that you want to export.

---

### **list**

lists all the traffic capture files that have been saved to date.

---

### **remove filename**

removes a packet capture file.

---

### **start filename zone-pair**

initiates the traffic capture between the designated zone pair and saves the capture to the specified file name. Traffic can only be captured between the zone pairs that are defined in the security zone profiles.

---

#### **-c**

an integer representing the number of packets that you want to capture.

#### **-C**

the maximum size, in megabytes, of the file to which you want to save the traffic capture information.

#### **-s**

source IP address.

#### **-d**

destination IP address.

#### **-D**

destination port number.

#### **-p**

IP protocol (such as UDP, ICMP, IGMP, TCP).

---

### **stop**

stops the current packet capture.

---

## **tree**

access: global; all

The tree command displays the command tree that is in effect from your current place in a menu or submenu. If you are at the main CLI prompt (**hostname#**) the command will display the entire command tree. If you are at a submenu prompt — such as **hostname (cfg-session) #** — the command tree available from that submenu displays.

The **-syntax** option adds syntax information to the command tree.

*view tree  
(command  
hierarchy)*

Use **tree** to view the command tree.

```
hostname# (cfg-session)# tree
session
|
+---alias
|
+---boot
|   |
|   +---list-image
|   |
|   +---remove-image
|   |
|   +---rollback
|
|bugreport
(continued)
```

*view tree  
(command  
hierarchy)  
with syntax  
notation*

Use **tree -syntax** to view the command tree with syntax notation.

```
hostname(cfg-session)# tree -syntax
session
|
+---columns <columns>
|
+---more
      no more
|
+---rows <rows>
|
+---timeout <minutes> [-persist]
|
+---wraparound
      no wraparound
```

## who

access: global; all

The **who** command displays the usernames, the connection methods, the IP addresses, and the login times of the users who are currently logged in on the device. By default, the login time is shown in local time, if you use the **-utc** option, the login time will be shown in Universal Time.

*list usernames  
and IP  
addresses of  
current users*

```
hostname# who
User                               I/F    IP Address      Login <Local Time>
=====
ekwalker                           CON    Serial          2003-8-18 10:28:17
kscanlon                           HTTP   111.222.33.66   2003-8-15 15:50:18
sserur                             HTTP   111.222.34.77   2003-8-16 11:40:04
ntulsian                           HTTP   111.222.35.88   2003-8-16 16:56:47
jkrejca                             HTTP   111.222.36.99   2003-8-17 16:48:30
```

### whoami

access: global; all

The **whoami** command lists the username, access role, and current path of the logged in user.

*list your user  
information*

```
hostname# whoami
User name: sysadmin
Role: super-user
SSH: 1.2.3.4
Login: 2003-08-26 11:56:06
```

# 4 Navigation

*Describes the X family Command Line Interface. This chapter details how to log in, issue commands, and use the CLI.*

## Overview

The Command Line Interface (CLI) is a standard embedded system command line interface that enables you to perform hardware configuration, software configuration, and monitoring activities.

## Logging in to the CLI

Log in to the CLI using an SSH session. To log in, you must meet the following requirements:

- SSH is enabled on the X Family device
- You have access to an SSH client
- A valid username and password are configured. If you do not have a username and password, a user with super-user access must create a user login and password for you.

### To Log in to the CLI

**STEP 1** Start an SSH session using the IP address of the device.

**STEP 2** Enter your user name at the **Login** prompt.

**STEP 3** Enter your password at the **Password** prompt.

# Navigation

The X family Command Line Interface offers the following features:

- [Command Types](#)
- [Hierarchical Submenus](#)
- [Command Hints](#)
- [Command Completion](#)
- [Command Help](#)
- [Command Aliases](#)

Each of these features is described below.

## Command Types

The CLI has two types of commands.

- **Global commands:** Available from within any menu level in the CLI. Global commands do not report on or change configuration items.
- **Hierarchal commands:** Available only within a menu or submenu.

## Hierarchical Submenus

The CLI divides commands into functional areas. There are several commands that lead to submenus, including **boot**, **configure terminal**, and **show**.

## Context Sensitive Prompt

The X family device prompt indicates what menu level you are currently using. The top-level menu prompt is:

```
hostname#
```

When you enter a submenu, the prompt indicates the current menu level in parentheses. For example, entering the **boot** command changes the CLI prompt to:

```
hostname (boot) #
```

## Exiting Submenus

The **exit** command steps back to the previous menu, or up one submenu. The **exit all** command returns you to the **hostname#** menu level.

## Command Hints

On each command level, you can view the hierarchical commands available at that level by typing a question mark (?). For example, when you are at the top level of the CLI:

```
hostname# ?
```

**Table 4–1: Command Hints**

| Command   | Description                                                                               |
|-----------|-------------------------------------------------------------------------------------------|
| boot      | Configures the OS image with which you want to boot.                                      |
| bugreport | Sends bug report email to designated destination                                          |
| configure | Configures hardware and software parameters.                                              |
| halt      | Halts system. Places the X family device into a state where it can be safely powered off. |
| reboot    | Reboots system.                                                                           |
| setup     | Starts running setup wizards.                                                             |
| show      | Shows system configuration, status, or statistics.                                        |
| snapshot  | Manages snapshots of the system.                                                          |

You can also enter the command **help commands** to show all the global commands that are available.

## Command Completion

The CLI attempts to match partially typed commands with valid commands. For example, if you type:

```
hostname# bo?
```

The CLI interprets this command as if you typed the following:

```
hostname# boot
```



**Note:** You can also use the Tab key for command completion.

## Command Help

At the CLI prompt, you can access the help topics for commands. At the prompt, type help:

```
hostname# help
```

The following information and options appears:

Global Commands:

|         |                                     |
|---------|-------------------------------------|
| alias   | Create command alias                |
| clear   | Reset system functions              |
| cls     | Clear screen                        |
| exit    | Exit intermediate mode              |
| help    | Show command help                   |
| history | Show command history                |
| logout  | Log off system                      |
| ping    | Send echo message                   |
| quit    | Log off system                      |
| tree    | Show command tree                   |
| who     | Show users currently logged in      |
| whoami  | Display current session information |

help commands Show only global commands

help edit Show editing keys

help displays information only on global commands.

For help on intermediate mode commands, type '?' at the base level of the command tree.

Type ' ?' at the end of a command for parameter information.

Commands that enable a feature or hardware component usually have a corresponding "no" command to disable it. For example:

- "configure terminal clock dst" enables daylight time.
- "configure terminal clock no dst" disables daylight time.

To see global commands, type **help commands**:

```
hostname# help commands
alias      Create command alias
clear      Reset system functions
cls        Clear screen
exit       Exit intermediate mode
help       Show command help
history    Show command history
logout     Log off system
ping       Send echo message
quit       Log off system
tree       Show command tree
who        Show users currently logged in
whoami     Display current session information
```

To see edit keys, type **help edit**:

```
hostname# help edit
Available editing keystrokes

Delete current character.....Ctrl-d
Delete text up to cursor.....Ctrl-u
Delete from cursor to end of line.....Ctrl-k
Move to beginning of line.....Ctrl-a
Move to end of line.....Ctrl-e
Get prior command from history.....Ctrl-p
Get next command from history.....Ctrl-n
Move cursor left.....Ctrl-b
Move cursor right.....Ctrl-f
Move back one word.....Esc-b
Move forward one word.....Esc-f
Convert rest of word to uppercase.....Esc-c
Convert rest of word to lowercase.....Esc-l
Delete remainder of word.....Esc-d
Delete word up to cursor.....Ctrl-w
Transpose current and previous character....Ctrl-t
Enter command and return to root prompt.....Ctrl-z
Refresh input line.....Ctrl-l
```

## Command Line Editing

In addition to the commands listed in the previous section, the following commands can be used to edit your command line entries:

**Table 4-2: CLI Edit Commands**

| Key Combination | Edit Function                                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------------------------|
| up arrow        | Enters the last command in the command line                                                                     |
| !! <cr>         | Executes the last command                                                                                       |
| !<number>       | Executes command number <number> in the history buffer. Use the <b>history</b> command to view command numbers. |

## Command Aliases

The CLI allows you to create aliases for long or complex command line entries. An alias is a string that can represent any of the following:

- a command
- a command parameter
- a command flag
- a combination of command, parameters, and flags

An alias that defines an entire command string can only be used to replace that command string, while an alias that defines a part of a command or a command parameter can be combined with additional command parameters.

**Table 4–3: Alias Definition Examples**

| define alias                      | before alias                | after alias       |
|-----------------------------------|-----------------------------|-------------------|
| alias s31 "show conf int eth 3 1" | show conf int eth 3 1       | s31               |
| alias 31 "int eth 3 1"            | show conf int eth 3 1       | show conf 31      |
|                                   | conf t int eth 3 1 shutdown | conf t 31 shut    |
| alias eth "int eth"               | show conf int eth 3 1       | show conf eth 3 1 |
|                                   | show conf int eth 3 1       | show conf eth 3 1 |
| alias sc "show conf"              | show conf int eth 3 1       | sc int eth 3 1    |
|                                   | show conf clock             | sc clock          |

## Console Settings

The CLI contains commands to configure how your terminal session behaves. The following table lists the default terminal settings and the CLI commands that you can use to change the settings.

**Table 4–4: Default Console Settings**

| Setting    | Description                                                                | Default Value | Command to Change Setting                  |
|------------|----------------------------------------------------------------------------|---------------|--------------------------------------------|
| columns    | sets the width of the session window in number of columns                  | 80            | conf t session col <number of columns>     |
| rows       | sets the height of the session window in number of columns                 | 25            | conf t session row <number of rows>        |
| more       | when enabled, displays large amounts of information in page-by-page format | on            | conf t session no more                     |
| wraparound | when enabled, wraps lines of text                                          | on            | conf t session no wrap                     |
| timeout    | sets the period of inactivity after which a user will be logged off        | 20 minutes    | conf t session timeout <number of minutes> |

See the command [“conf t session” on page 65](#) for more information.



**Note:** The timeout persists only if the -persist option is used when configuring the terminal session timeout. The timeout -persist option requires super-user privileges.



**Tip:** For best viewing, be sure to set your terminal software's row and column settings to match your CLI session's row and column settings.



# Index

! 28

## A

- account security 4
- action sets 22, 87
- additional configuration 16
- address groups 26
- alert sink 40, 93
- alias 27, 28, 127
- application protection 60, 91, 111
- ARP table 87
- authentication 36
  - privilege groups 27

## B

- boot 27, 29
- bugreport 30

## C

- category settings 21, 38
- chassis 87
- clear 31
- clock 7, 24, 38, 58, 88, 115
- cls 33
- CMOS 3, 8
- command overview 21
- commands
  - abbreviating 28
  - aliases 127
  - completing 125
  - editing 127
  - executing 28
  - help 126
  - hints 125
- configuration 2, 16, 33, 86
- configure 33
  - terminal
    - monitor threshold 57
  - nms
    - community 58
    - ip 58
    - no nms 58

- configure terminal 33
  - address-group 35
  - authentication 36
  - autodv 37
  - category-settings 38
  - clock 38
  - default-alert-sink 40
  - default-gateway 41
  - dhcp-server 41
  - dns 43
  - email-rate-limit 43
  - filter 44
  - firewall rule 45
  - firewall schedule 47
  - firewall service 48
  - firewall service-group 48
  - firewall virtual-server 49
- interface 50
  - ethernet 50
  - external virtual 51
  - GRE virtual 53
  - internal virtual 54
  - remove virtual 55
  - settings 51
  - virtual 51
- local-user 55
- log audit select 56
- nms 58
  - notify-contact 58
- ntp 58
- port 59
- protection-settings 60
- ramdisk 61
- routing 63
- server 64
- service-access 64
- session 65
- sms 66
- tse 67
- user 67
- vpn ike 71
- vpn ipsec 74
- vpn l2tp 76
- vpn pptp 77
- web-filtering 78
- zone 80

- console settings 128
- content filtering 78
- context sensitive prompt 124
- counters
  - clearing 31
  - policy 111
- customer support viii, 30, 64, 81, 114

## D

- daylight saving time 3, 8

- debug 81
  - factory-reset 81
  - log syslog 81
- default email contact 18, 19
- default gateway 26, 41, 93
- DHCP server 26, 41, 93
- Digital Vaccine 24, 37, 87
- disk space 95
- DNS 26, 43
- DST 3

## E

- email alerts 18
- email notification 18, 43, 58, 91
- ethernet port 17
  - auto negotiation 18
  - duplex setting 18
  - line speed 18
- exit 81

## F

- filter 44, 94
- filter categories 38
- firewall 22
  - rules 45, 94
  - schedules 47
  - service groups 48
  - services 48
  - sessions 94
  - virtual servers 49

## G

- guide
  - audience vi
  - caution vii
  - conventions vi
  - note viii
  - tip viii
  - warning vii

## H

- halt 82
- health 23, 95
- help 82
- hierarchical submenus 124
  - context sensitive prompt 124
  - exiting 124
- high-availability 24, 82, 96
- history 27, 28, 83
- HTTP 3, 14, 15, 64
- HTTPS 3, 14, 15, 64

**I**

images 29  
 infrastructure protection 60, 91, 111  
 interface 26  
   ethernet 50, 90, 96  
   external virtual 51  
   GRE virtual 53  
   internal virtual 54  
   management port 90, 96  
   removing 55  
   settings 51, 91  
   virtual 51, 91, 96  
 interfaces 50  
 IP address groups 35  
 IPS services 22

**L**

local user 55  
 log 23, 91, 98  
   alert 99  
   audit 56, 99  
   block 100  
   clearing 31  
   firewall session 100  
   firewallblock 100  
   system 100  
   VPN 101  
 logout 83

**M**

management port 41  
 memory 95

**N**

navigation  
   context sensitive prompt 124  
   hierarchical submenus 124  
   hints 125  
 Network Monitoring System (NMS) 3, 16,  
   24, 58  
 network processor statistics 101  
 NMS 16  
 NTP 3, 8, 58

**P**

performance protection 60, 91, 111  
 ping 84  
 policy counters 111  
 port 25, 59  
   clearing 31  
 privilege groups 27, 36  
 protection settings 91, 111

**Q**

quit 85

**R**

RADIUS 27, 36  
 RAM disk statistics 112  
 RAM disk synchronization 61, 91  
 reboot 85  
 related documentation viii  
 remote deployment 13  
 reset 81  
 rollback 29  
 routing 26, 63, 113

**S**

screen, clearing 33  
 security 4  
 Security Management System (SMS) 13,  
   16, 24, 66, 92, 115  
   remote deployment 13  
 security zones 25  
 server 114  
 server options 92  
   CLI 14  
   default settings 15  
   HTTP 15  
   HTTPS 15  
   non-secure 14  
   secure 14  
   SMS 14  
   SNMP 14, 15  
   SSH 15  
   web 14  
 service access 64, 114  
 session 27, 65, 92, 114  
 setup 25, 86  
 setup wizard 25  
   additional config 16  
   additional configuration 2  
   terminal 2  
 show 86  
   action-sets 87  
   arp 87  
   autodv 87  
   chassis 87  
   clock 88  
   configuration  
     high-availability 89  
     interface 90  
   default-alert-sink 93  
   default-gateway 93  
   dhcp-server 93  
   filter 94  
   firewall rules 94  
   firewall sessions 94  
   health 95  
   high-availability 96  
   interface 96  
     ethernet 96  
     mgmtEthernet 96  
     virtual 96  
   log 98  
     alert 99  
     audit 99  
     block 100  
     firewallblock 100  
     firewallsession 100  
     system 100  
     vpn 101  
   np 101  
   policy counters 111  
   protection-settings 111  
   ramdisk 112  
   routing 113  
   server 114  
   service-access 114  
   session 114  
   sms 115  
   timezones 115  
   tse 116  
   user 116  
   version 117  
   vpn 117  
 show configuration 88  
   interface  
     ethernet 90  
     mgmtEthernet 90  
     settings 91  
     virtual 91  
   log 91  
   notify-contacts 91  
   protection-settings 91  
   ramdisk 91  
   remote-syslog 91  
   server 92  
   session 92  
   sms 92  
   tse 92  
   user 92  
 snapshot 118  
 SNMP 15  
 SSH 3, 14, 15, 64  
 super-user 5  
 syslog server 25, 81, 91

## T

- tech support viii
- temperature 95
- terminal setup wizard 2, 20
  - account security 4
  - configuration settings 2
  - NMS 16
  - super-user 5
  - timekeeping 7
  - web/CLI/SNMP 14
- Threat Management Center (TMC) viii
- Threat Suppression Engine (TSE) 24, 67, 92, 116
- time zone 8, 115
- timekeeping 7, 24, 38, 58, 88, 115
  - daylight saving time 8
  - NTP 8
  - peer time server 8
  - time server 8
  - time zone 8
- traceroute 118
- traffic-capture 119
- tree 120
- troubleshooting 30, 81

## U

- user 26, 55, 67, 92, 116

## V

- version number 117
- VPN 23, 101, 117
  - IKE 71
  - IPSec 74
  - L2TP 76
  - PPTP 77

## W

- web filtering 78
- who 121
- whoami 122

